ORAL ARGUMENT NOT YET SCHEDULED

No. 17-5171

IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER
Plaintiff-Appellant,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,
Defendants-Appellees.

On Appeal from an Order of the
U.S. District Court for the District of Columbia
Case No. 17-cv-1320(CKK)

JOINT APPENDIX

MARK B. STERN
DANIEL TENNY
Attorneys, Appellate Staff
Civil Division
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
(202) 514-1838
Counsel for Defendants-Appellees

MARC ROTENBERG
ALAN BUTLER
CAITRIONA FITZGERALD
JERAMIE SCOTT
JOHN DAVISSON
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Plaintiff-Appellant

INDEX TO JOINT APPENDIX

Page

Exhibits to Plaintiff's Amended Motion (ECF No. 35):

APPEAL,TYPE-D

U.S. District Court
District of Columbia (Washington, DC)
CIVIL DOCKET FOR CASE #: 1:17-cv-01320-CKK

ELECTRONIC PRIVACY INFORMATION CENTER v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY et al
Assigned to: Judge Colleen Kollar-Kotelly
Cases: 1:17-cv-01351-CKK
1:17-cv-01354-CKK
Case in other court: USCA, 17-05171
Cause: 05:702 Administrative Procedure Act

Date Filed: 07/03/2017
Jury Demand: None
Nature of Suit: 899 Administrative Procedure Act/Review or Appeal of Agency Decision
Jurisdiction: U.S. Government Defendant

Plaintiff

ELECTRONIC PRIVACY INFORMATION CENTER

represented by **Marc Rotenberg**
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140, ext 106
Fax: (202) 483-1248
Email: rotenberg@epic.org
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Alan Jay Butler
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140 ext 103
Fax: (202) 483-1248
Email: butler@epic.org
ATTORNEY TO BE NOTICED

Caitriona Fitzgerald
ELECTRONIC PRIVACY INFORMATION CENTER
14 Tyler Street
Third Floor
Somerville, MA 02143

(617) 94508409
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jeramie D. Scott
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140
Fax: (202) 483-1248
Email: jscott@epic.org
ATTORNEY TO BE NOTICED

V.

Defendant

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY

represented by

Carol Federighi
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
(202) 514-1903
Email: carol.federighi@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
(202) 514-5302
Fax: (202) 616-8202
Email: Elizabeth.Shapiro@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
U.S. DEPARTMENT OF JUSTICE
P.O. Box 883
Washington, DC 20044
(202) 514-1944
Fax: (202) 616-8460
Email: joseph.borson@usdoj.gov
LEAD ATTORNEY

ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
US DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
Suite 7000
Washington, DC 20001
(202) 353-4519
Email: kristina.wolfe@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

MICHAEL PENCE
In his official capacity as Chair of the Presidential Advisory Commission on Election Integrity

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

KRIS KOBACH
In his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)

LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)

LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

GENERAL SERVICES ADMINISTRATION

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

U.S. DEPARTMENT OF DEFENSE

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

CHARLES G. HERNDON
in his official capacity as Director of White House Information Technology

represented by **Joseph Evan Borson**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

UNITED STATES DIGITAL SERVICE represented by **Kristina Ann Wolfe**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY represented by **Joseph Evan Borson**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
07/03/2017	1	COMPLAINT against EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY (Filing fee $ 400, receipt number 4616085803) filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Civil Cover Sheet)(td) (Entered: 07/03/2017)
07/03/2017		SUMMONS (8) Issued as to EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, U.S. Attorney and U.S. Attorney General (td) (Entered: 07/03/2017)
07/03/2017	2	LCvR 7.1 CERTIFICATE OF DISCLOSURE of Corporate Affiliations and Financial Interests by ELECTRONIC PRIVACY INFORMATION CENTER (td) (Entered: 07/03/2017)
07/03/2017	3	MOTION for Temporary Restraining Order by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Exhibit, # 2 Text of Proposed Order)(td) (Entered: 07/03/2017)
07/03/2017		MINUTE ORDER: At approximately 4:50 P.M. EST, the Court held an on-the-record teleconference, attended by counsel for both parties, to set a briefing schedule on Plaintiff's 3 Emergency Motion for a Temporary Restraining Order. Defendants shall file their opposition to the motion by 4 P.M. EST on WEDNESDAY, JULY 5, 2017. Plaintiff shall file its reply by 9 A.M. EST on THURSDAY, JULY 6, 2017. Signed by Judge Colleen Kollar-Kotelly on 7/3/2017. (lcckk1) (Entered: 07/03/2017)
07/03/2017	4	ORDER Establishing Procedures for Cases Assigned to Judge Colleen Kollar-Kotelly.

		Signed by Judge Colleen Kollar-Kotelly on 07/03/2017. (DM) (Entered: 07/03/2017)
07/03/2017	5	NOTICE of Appearance by Elizabeth J. Shapiro on behalf of All Defendants (Shapiro, Elizabeth) (Entered: 07/03/2017)
07/03/2017		Minute Entry for proceedings held before Judge Colleen Kollar-Kotelly: Telephone Conference held on 7/3/2017. (Court Reporter Richard Ehrlich.) (dot) (Entered: 07/07/2017)
07/05/2017	6	NOTICE of Appearance by Carol Federighi on behalf of All Defendants (Federighi, Carol) (Entered: 07/05/2017)
07/05/2017	7	NOTICE of Appearance by Joseph Evan Borson on behalf of EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY (Borson, Joseph) (Entered: 07/05/2017)
07/05/2017	8	RESPONSE re 3 MOTION for Temporary Restraining Order filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Attachments: # 1 Declaration of Kris Kobach, # 2 Text of Proposed Order)(Federighi, Carol) (Entered: 07/05/2017)
07/05/2017	9	ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/5/2017. (lcckk1) (Entered: 07/05/2017)
07/06/2017	10	TRANSCRIPT OF SCHEDULING CONFERENCE before Judge Colleen Kollar-Kotelly held on July 3, 2017; Page Numbers: 1- 13. Date of Issuance: July 6, 2017. Court Reporter/Transcriber Richard D. Ehrlich, Telephone number 202-354-3269, Transcripts may be ordered by submitting the Transcript Order Form For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi-page, condensed, CD or ASCII) may be purchased from the court reporter. **NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty-one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov. Redaction Request due 7/27/2017. Redacted Transcript Deadline set for 8/6/2017. Release of Transcript Restriction set for 10/4/2017.(Ehrlich, Richard) Modified date of hearing on 7/7/2017 (znmw). (Entered: 07/06/2017)
07/06/2017	11	RESPONSE TO ORDER OF THE COURT re 9 Order filed by EXECUTIVE OFFICE

		OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Attachments: # 1 Declaration of Kris W. Kobach)(Borson, Joseph) (Entered: 07/06/2017)
07/06/2017	12	NOTICE of Appearance by Alan Jay Butler on behalf of ELECTRONIC PRIVACY INFORMATION CENTER (Butler, Alan) (Entered: 07/06/2017)
07/06/2017	13	REPLY to opposition to motion re 3 MOTION for Temporary Restraining Order filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Addendum, # 2 Affirmation of Marc Rotenberg, # 3 Exhibits 1-11)(Butler, Alan) (Entered: 07/06/2017)
07/06/2017	14	ERRATA by ELECTRONIC PRIVACY INFORMATION CENTER 13 Reply to opposition to Motion filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Corrected Exhibit 11)(Butler, Alan) (Entered: 07/06/2017)
07/06/2017	15	ORDER. The Court hereby sets a hearing on Plaintiff's 3 Motion for a Temporary Restraining Order, to be held at 4:00 P.M. on July 7, 2017, in Courtroom 28A. Signed by Judge Colleen Kollar-Kotelly on 7/6/2017. (lcckk1) (Entered: 07/06/2017)
07/06/2017		Set/Reset Hearings: Motion Hearing set for 7/7/2017 at 4:00 PM in Courtroom 28A before Judge Colleen Kollar-Kotelly. (dot) (Entered: 07/07/2017)
07/07/2017	16	Unopposed MOTION for Leave to File *Surreply* by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY (Attachments: # 1 Exhibit Proposed Surreply, # 2 Text of Proposed Order)(Federighi, Carol) (Entered: 07/07/2017)
07/07/2017	17	RESPONSE TO ORDER OF THE COURT *Filing of Supplemental Brief* by ELECTRONIC PRIVACY INFORMATION CENTER re 15 Order (Butler, Alan) Modified event title on 7/10/2017 (znmw). (Entered: 07/07/2017)
07/07/2017	18	RESPONSE TO ORDER OF THE COURT re 15 Order *Defendants' Supplemental Brief on Informational Standing* filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Borson, Joseph) (Entered: 07/07/2017)
07/07/2017	19	Unopposed MOTION for Leave to File *Sur-surreply* by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Exhibit Proposed sur-surreply, # 2 Exhibit Exhibit to proposed sur-surreply, # 3 Text of Proposed Order)(Butler, Alan) (Entered: 07/07/2017)
07/07/2017	20	NOTICE *of Supplemental Exhibits* by ELECTRONIC PRIVACY INFORMATION CENTER re 15 Order (Attachments: # 1 Supplemental Exhibits)(Butler, Alan) (Entered: 07/07/2017)

07/07/2017		Minute Entry for proceedings held before Judge Colleen Kollar-Kotelly: Motion Hearing held on 7/7/2017 re 3 MOTION for Temporary Restraining Order filed by ELECTRONIC PRIVACY INFORMATION CENTER; and taken under advisement. (Court Reporter Richard Ehrlich.) (dot) (Entered: 07/07/2017)
07/07/2017	21	AMENDED COMPLAINT *pursuant to FRCP 15(a)(1)(A)* against ELECTRONIC PRIVACY INFORMATION CENTER filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Summons as to U.S. Department of Defense)(Butler, Alan) (Entered: 07/07/2017)
07/09/2017	22	TRANSCRIPT OF TEMPORARY RESTRAINING ORDER before Judge Colleen Kollar-Kotelly held on July 7, 2017; Page Numbers: 1 - 63. Date of Issuance:July 10, 2017. Court Reporter/Transcriber Richard D. Ehrlich, Telephone number (202) 354-3269, Transcripts may be ordered by submitting the Transcript Order Form For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased fro m the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi-page, condensed, CD or ASCII) may be purchased from the court reporter. **NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty-one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov. Redaction Request due 7/30/2017. Redacted Transcript Deadline set for 8/9/2017. Release of Transcript Restriction set for 10/7/2017.(Ehrlich, Richard) (Entered: 07/09/2017)
07/10/2017	23	ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/10/2017. (lcckk1) (Entered: 07/10/2017)
07/10/2017		Set/Reset Deadline: Supplemental briefing due by 4:00 PM on 7/10/2017. (tth) (Entered: 07/10/2017)
07/10/2017	24	RESPONSE TO ORDER OF THE COURT re 23 Order *Supplemental Brief re: DOD* filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Attachments: # 1 Declaration Third Kobach Decl.)(Borson, Joseph) (Entered: 07/10/2017)
07/10/2017	25	SUMMONS (1) Issued Electronically as to U.S. DEPARTMENT OF DEFENSE. (znmw) (Entered: 07/10/2017)
07/10/2017	26	ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/10/2017. (lcckk1) (Entered:

		07/10/2017)
07/11/2017	27	RESPONSE TO ORDER OF THE COURT re 26 Order filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Butler, Alan) (Entered: 07/11/2017)
07/11/2017	28	NOTICE of Appearance by Jeramie D. Scott on behalf of ELECTRONIC PRIVACY INFORMATION CENTER (Scott, Jeramie) (Entered: 07/11/2017)
07/11/2017	29	MOTION for Leave to Appear Pro Hac Vice :Attorney Name- Caitriona Fitzgerald, :Firm- Electronic Privacy Information Center, :Address- 14 Tyler Street, Third Floor, Somerville, MA 02143. Phone No. - (617) 945-8409. Filing fee $ 100, receipt number 0090-5026343. Fee Status: Fee Paid. by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Declaration of Caitriona Fitzgerald, # 2 Text of Proposed Order)(Rotenberg, Marc) (Entered: 07/11/2017)
07/11/2017	30	MOTION for Leave to File *a Second Amended Complaint* by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Second Amended Complaint, # 2 Exhibit 5, # 3 Summons as to Charles C. Herndon, # 4 Summons as to U.S. Digital Service, # 5 Summons as to Executive Committee for Presidential Information Technology, # 6 Text of Proposed Order)(Butler, Alan) (Entered: 07/11/2017)
07/11/2017	31	ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/11/2017. (lcckk1) (Entered: 07/11/2017)
07/11/2017	32	RESPONSE re 30 MOTION for Leave to File *a Second Amended Complaint* filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, U.S. DEPARTMENT OF DEFENSE. (Federighi, Carol) (Entered: 07/11/2017)
07/11/2017		MINUTE ORDER: For good cause shown, and in light of Defendants' notice that they do not oppose this relief, ECF No. 32, Plaintiff's 30 Motion for Leave to File a Second Amended Complaint is GRANTED. Signed by Judge Colleen Kollar-Kotelly on 7/11/2017. (lcckk1) (Entered: 07/11/2017)
07/11/2017	33	SECOND AMENDED COMPLAINT against GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, U.S. DEPARTMENT OF DEFENSE, CHARLES G. HERNDON, UNITED STATES DIGITAL SERVICE, EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Exhibit 5) (znmw) (Entered: 07/12/2017)
07/12/2017	34	SUMMONS (3) Issued Electronically as to EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY, CHARLES G. HERNDON, UNITED STATES DIGITAL SERVICE. (znmw) (Entered: 07/12/2017)
07/13/2017	35	Amended MOTION for Temporary Restraining Order , MOTION for Preliminary Injunction by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1

		Memorandum in Support, # 2 Exhibit List, # 3 Exhibit 1-20, # 4 Exhibit 21-30, # 5 Exhibit 31-40, # 6 Text of Proposed Order)(Butler, Alan) (Entered: 07/13/2017)
07/13/2017	36	ERRATA *Corrected Exhibits 21-30* by ELECTRONIC PRIVACY INFORMATION CENTER 35 Amended MOTION for Temporary Restraining Order MOTION for Preliminary Injunction filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Exhibit 21-30)(Butler, Alan) (Entered: 07/13/2017)
07/16/2017	37	NOTICE of Appearance by Kristina Ann Wolfe on behalf of All Defendants (Wolfe, Kristina) (Entered: 07/16/2017)
07/17/2017	38	RESPONSE re 35 Amended MOTION for Temporary Restraining Order MOTION for Preliminary Injunction filed by EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY, EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, CHARLES G. HERNDON, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE. (Attachments: # 1 Declaration, # 2 Text of Proposed Order)(Borson, Joseph) (Entered: 07/17/2017)
07/17/2017	39	REPLY to opposition to motion re 35 Amended MOTION for Temporary Restraining Order MOTION for Preliminary Injunction filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Declaration of Eleni Kyriakides)(Butler, Alan) (Entered: 07/17/2017)
07/18/2017		NOTICE OF ERROR re 39 Reply to opposition to Motion; emailed to butler@epic.org, cc'd 9 associated attorneys -- The PDF file you docketed contained errors: 1. FYI on future filings, the signature of the person filing and the one signing the document must match. (ztd,) (Entered: 07/18/2017)
07/24/2017	40	MEMORANDUM OPINION. Signed by Judge Colleen Kollar-Kotelly on 7/24/2017. (lcckk1) (Entered: 07/24/2017)
07/24/2017	41	ORDER. Plaintiff's 35 Motion for a Temporary Restraining Order and Preliminary Injunction is DENIED WITHOUT PREJUDICE. Signed by Judge Colleen Kollar-Kotelly on 7/24/2017. (lcckk1) (Entered: 07/24/2017)
07/25/2017	42	NOTICE OF APPEAL TO DC CIRCUIT COURT as to 41 Order on Motion for TRO, Order on Motion for Preliminary Injunction by ELECTRONIC PRIVACY INFORMATION CENTER. Filing fee $ 505, receipt number 0090-5047166. Fee Status: Fee Paid. Parties have been notified. (Attachments: # 1 Exhibit 1)(Rotenberg, Marc) (Entered: 07/25/2017)
07/26/2017	43	Transmission of the Notice of Appeal, Order Appealed (Memorandum Opinion), and Docket Sheet to US Court of Appeals. The Court of Appeals fee was paid this date re 42 Notice of Appeal to DC Circuit Court. (znmw) (Entered: 07/26/2017)
07/27/2017		USCA Case Number 17-5171 for 42 Notice of Appeal to DC Circuit Court, filed by ELECTRONIC PRIVACY INFORMATION CENTER. (zrdj) (Entered: 07/27/2017)
08/02/2017	44	RETURN OF SERVICE/AFFIDAVIT of Summons and Complaint Executed as to the United States Attorney. Date of Service Upon United States Attorney on 7/16/2017.

		Answer due for ALL FEDERAL DEFENDANTS by 9/4/2017. (Rotenberg, Marc) Modified dates on 8/3/2017 (znmw). (Entered: 08/02/2017)
08/02/2017	45	RETURN OF SERVICE/AFFIDAVIT of Summons and Complaint Executed on United States Attorney General. Date of Service Upon United States Attorney General 7/6/2017. (Rotenberg, Marc) Modified date of service on 8/3/2017 (znmw). (Entered: 08/02/2017)
08/02/2017	46	RETURN OF SERVICE/AFFIDAVIT of Summons and Complaint Executed. EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY served on 7/24/2017; EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES served on 7/6/2017; GENERAL SERVICES ADMINISTRATION served on 7/6/2017; CHARLES G. HERNDON served on 7/24/2017; KRIS KOBACH served on 7/6/2017; OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES served on 7/6/2017; MICHAEL PENCE served on 7/6/2017; PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY served on 7/6/2017; U.S. DEPARTMENT OF DEFENSE served on 7/24/2017; UNITED STATES DIGITAL SERVICE served on 7/24/2017 (Rotenberg, Marc) (Entered: 08/02/2017)
08/11/2017		MINUTE ORDER: The 3 Motion for Temporary Restraining Order and related 16 Motion for Leave to File Surreply, and 17 Motion for Leave to File Sur-surreply, are DENIED AS MOOT. The Court previously ordered Plaintiff to file an amended motion for injunctive relief. Order, ECF No. 31. The 35 Amended Motion for Temporary Restraining Order and Preliminary Injunction was resolved by the Court's July 24, 2017 Memorandum Opinion, ECF No. 40. Separately, the Court has received the 29 Motion for Admission Pro Hac Vice of attorney Caitriona Fitzgerald. That Motion is GRANTED CONTINGENT on Ms. Fitzgerald filing a declaration, by AUGUST 18, 2017, certifying to the Court that she is familiar with the Local Rules of this Court. (lcckk1) (Entered: 08/11/2017)
08/16/2017	47	RESPONSE TO ORDER OF THE COURT re Order on Motion for Leave to Appear Pro Hac Vice,,,, Order on Motion for TRO,,,, Order on Motion for Leave to File,,,,,,, filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Declaration of Caitriona Fitzgerald)(Butler, Alan) (Entered: 08/16/2017)

PACER Service Center			
Transaction Receipt			
08/17/2017 21:15:12			
PACER Login:	ep0116:2545265:0	**Client Code:**	
Description:	Docket Report	**Search Criteria:**	1:17-cv-01320-CKK

Billable Pages:	10	**Cost:**	1.00

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,
Plaintiff,
v.
PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,
Defendants.

Civil Action No. 17-1320 (CKK)

MEMORANDUM OPINION
(July 24, 2017)

This case arises from the establishment by Executive Order of the Presidential Advisory Commission on Election Integrity (the "Commission"), and a request by that Commission for each of the 50 states and the District of Columbia to provide it with certain publicly available voter roll information. Pending before the Court is Plaintiff's [35] Amended Motion for Temporary Restraining Order and Preliminary Injunction, which seeks injunctive relief prohibiting Defendants from "collecting voter roll data from states and state election officials" and directing Defendants to "delete and disgorge any voter roll data already collected or hereafter received." Proposed TRO, ECF No. 35-6, at 1-2.

Although substantial public attention has been focused on the Commission's request, the legal issues involved are highly technical. In addition to the Fifth Amendment of the Constitution, three federal laws are implicated: the Administrative Procedure Act, 5 U.S.C. § 551 *et seq.* ("APA"), the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 ("E-Government Act"), and the Federal Advisory Committee Act, codified at 5 U.S.C. app. 2 ("FACA"). All three are likely unfamiliar to the vast majority of Americans, and even seasoned legal practitioners are unlikely to have encountered the latter two.

Matters are further complicated by the doctrine of standing, a Constitutional prerequisite for this Court to consider the merits of this lawsuit.

Given the preliminary and emergency nature of the relief sought, the Court need not at this time decide conclusively whether Plaintiff is, or is not, ultimately entitled to relief on the merits. Rather, if Plaintiff has standing to bring this lawsuit, then relief may be granted if the Court finds that Plaintiff has a likelihood of succeeding on the merits, that it would suffer irreparable harm absent injunctive relief, and that other equitable factors—that is, questions of fairness, justice, and the public interest—warrant such relief.

The Court held a lengthy hearing on July 7, 2017, and has carefully reviewed the parties' voluminous submissions to the Court, the applicable law, and the record as a whole. Following the hearing, additional defendants were added to this lawsuit, and Plaintiff filed the pending, amended motion for injunctive relief, which has now been fully briefed. For the reasons detailed below, the Court finds that Plaintiff has standing to seek redress for the informational injuries that it has allegedly suffered as a result of Defendants declining to conduct and publish a Privacy Impact Assessment pursuant to the E-Government Act prior to initiating their collection of voter roll information. Plaintiff does not, however, have standing to pursue Constitutional or statutory claims on behalf of its advisory board members.

Although Plaintiff has won the standing battle, it proves to be a Pyrrhic victory. The E-Government Act does not itself provide for a cause of action, and consequently, Plaintiff must seek judicial review pursuant to the APA. However, the APA only applies to "agency action." Given the factual circumstances presently before the Court—which have changed substantially since this case was filed three weeks ago—Defendants' collection of voter

roll information does not currently involve agency action. Under the binding precedent of this circuit, entities in close proximity to the President, which do not wield "substantial independent authority," are not "agencies" for purposes of the APA. On this basis, neither the Commission or the Director of White House Information Technology—who is currently charged with collecting voter roll information on behalf of the Commission—are "agencies" for purposes of the APA, meaning the Court cannot presently exert judicial review over the collection process. To the extent the factual circumstances change, however—for example, if the *de jure* or *de facto* powers of the Commission expand beyond those of a purely advisory body—this determination may need to be revisited. Finally, the Court also finds that Plaintiff has not demonstrated an irreparable informational injury—given that the law does not presently entitle it to information—and that the equitable and public interest factors are in equipoise. These interests may very well be served by additional disclosure, but they would not be served by this Court, without a legal mandate, ordering the disclosure of information where no right to such information currently exists. Accordingly, upon consideration of the pleadings,[1] the relevant legal authorities, and the record as a whole, Plaintiff's [35] Motion for a Temporary Restraining Order and Preliminary Injunction is **DENIED WITHOUT PREJUDICE**.[2]

---

[1] The Court's consideration has focused on the following documents:

- Mem. in Supp. of Pl.'s Am. Mot. for a TRO and Prelim. Inj., ECF No. 35-1 ("Pls. Am. Mem.");
- Defs.' Mem. in Opp'n to Pl.'s Am. Mot. for a TRO and Prelim. Inj., ECF No. 38 ("Am. Opp'n Mem.");
- Reply in Supp. of Pl.'s Am. Mot. for a TRO and Prelim. Inj., ECF No. 39 ("Am. Reply Mem.").

[2] For the avoidance of doubt, the Court denies without prejudice both Plaintiff's motion for a temporary restraining order, and its motion for a preliminary injunction.

I. BACKGROUND

The Commission was established by Executive Order on May 11, 2017. Executive Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017) ("Exec. Order"). According to the Executive Order, the Commission's purpose is to "study the registration and voting processes used in Federal elections." *Id.* § 3. The Executive Order states that the Commission is "solely advisory," and that it shall disband 30 days after submitting a report to the President on three areas related to "voting processes" in federal elections. *Id.* §§ 3, 6. The Vice President is the chair of the Commission, and the President may appoint 15 additional members. From this group, the Vice President is permitted to appoint a Vice Chair of the Commission. The Vice President has named Kris W. Kobach, Secretary of State for Kansas, to serve as the Vice Chair. Decl. of Kris Kobach, ECF No. 8-1 ("Kobach Decl."), ¶ 1. Apart from the Vice President and the Vice Chair, there are presently ten other members of the Commission, including Commissioner Christy McCormick of the Election Assistance Commission (the "EAC"), who is currently the only federal agency official serving on the Commission, and a number of state election officials, both Democratic and Republican, and a Senior Legal Fellow of the Heritage Foundation. *Lawyers' Committee for Civil Rights Under the Law v. Presidential Advisory Commission on Election Integrity*, No. 17-cv-1354 (D.D.C. July 10, 2017), Decl. of Andrew J. Kossack, ECF No. 15-1 ("Kossack Decl."), ¶ 1; Second Decl. of Kris W. Kobach, ECF No. 11-1 ("Second Kobach Decl."), ¶ 1. According to Defendants, "McCormick is not serving in her official capacity as a member of the EAC." Second Kobach Decl. ¶ 2. The Executive Order also provides that the General Services Administration ("GSA"), a federal agency, will "provide the Commission with such administrative services, funds, facilities, staff, equipment, and other

support services as may be necessary to carry out its mission on a reimbursable basis," and that other federal agencies "shall endeavor to cooperate with the Commission." Exec. Order, § 7.

Following his appointment as Vice Chair, Mr. Kobach directed that identical letters "be sent to the secretaries of state or chief election officers of each of the fifty states and the District of Columbia." Kobach Decl. ¶ 4. In addition to soliciting the views of state officials on certain election matters by way of seven broad policy questions, each of the letters requests that state officials provide the Commission with the "publicly available voter roll data" of their respective states, "including, if publicly available under the laws of [their] state, the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information." Kobach Decl., Ex. 3 (June 28, 2017 Letter to the Honorable John Merrill, Secretary of State of Alabama). The letters sent by Mr. Kobach also indicate that "[a]ny documents that are submitted to the full Commission will . . . be made available to the public." *Id.* Defendants have represented that this statement applies only to "narrative responses" submitted by states to the Commission. *Id.* ¶ 5. "With respect to voter roll data, the Commission intends to de-identify any such data prior to any public release of documents. In other words, the voter rolls themselves will not be released to the public by the Commission." *Id.* The exact process by which de-identification and publication of voter roll data will occur has yet to be determined. Hr'g Tr. 36:20–37:8.

Each letter states that responses may be submitted electronically to an email address, ElectionIntegrityStaff@ovp.eop.gov, "or by utilizing the Safe Access File Exchange ('SAFE'), which is a secure FTP site the federal government uses for transferring large data files." Kobach Decl., Ex. 3. The SAFE website is accessible at https://safe.amrdec.army.mil/safe/ Welcome.aspx. Defendants have represented that it was their intention that "narrative responses" to the letters' broad policy questions should be sent via email, while voter roll information should be uploaded by using the SAFE system. *Id.* ¶ 5.

According to Defendants, the email address named in the letters "is a White House email address (in the Office of the Vice President) and subject to the security protecting all White House communications and networks." *Id.* Defendants, citing security concerns, declined to detail the extent to which other federal agencies are involved in the maintenance of the White House computer system. Hr'g Tr. 35:2-10. The SAFE system, however, is operated by the U.S. Army Aviation and Missile Research Development and Engineering Center, a component of the Department of Defense. Second Kobach Decl. ¶ 4; Hr'g Tr. 32:6–9. The SAFE system was "originally designed to provide Army Missile and Research, Development and Engineering Command (AMRDEC) employees and those doing business with AMRDEC an alternate way to send files." Safe Access File Exchange (Aug. 8, 2012), *available at* http://www.doncio.navy.mil/ContentView.aspx?id=4098 (last accessed July 20, 2017). The system allows "users to send up to 25 files securely to recipients within the .mil or .gov domains[,]" and may be used by anyone so long as the recipient has a .mil or .gov email address. After an individual uploads data via the SAFE system, the intended recipient receives an email message indicating that "they have been

given access to a file" on the system, and the message provides instructions for accessing the file. The message also indicates the date on which the file will be deleted. This "deletion date" is set by the originator of the file, and the default deletion date is seven days after the upload date, although a maximum of two weeks is permitted.

Defendants portrayed the SAFE system as a conduit for information. Once a state had uploaded voter roll information via the system, Defendants intended to download the data and store it on a White House computer system. Second Kobach Decl. ¶ 5. The exact details of how that would happen, and who would be involved, were unresolved at the time of the hearing. Hr'g Tr. 34:3–35:10; 35:23–36:9. Nonetheless, there is truth to Defendants' description. Files uploaded onto the system are not archived after their deletion date, and the system is meant to facilitate the transfer of files from one user to another, and is not intended for long-term data storage. As Defendants conceded, however, files uploaded onto the SAFE system are maintained for as many as fourteen days on a computer system operated by the Department of Defense. Hr'g Tr. 31:7–32:5; 36:1–9 (The Court: "You seem to be indicating that DOD's website would maintain it at least for the period of time until it got transferred, right?" Ms. Shapiro: "Yes. This conduit system would have it for – until it's downloaded. So from the time it's uploaded until the time it's downloaded for a maximum of two weeks and shorter if that's what's set by the states."). Defendants stated that as, of July 7, only the state of Arkansas had transmitted voter roll information to the Commission by uploading it to the SAFE system. Hr'g Tr. 40:10–18. According to Defendants, the Commission had not yet downloaded Arkansas' voter data; and as of the date of the hearing, the data continued to reside on the SAFE system. *Id.*

Shortly after the hearing, Plaintiff amended its complaint pursuant to Federal Rule

of Civil Procedure 15(a)(1)(A), and added the Department of Defense as a defendant. Am. Compl., ECF No. 21. The Court then permitted Defendants to file supplemental briefing with respect to any issues particular to the Department of Defense. Order, ECF No. 23. On July 10, Defendants submitted a Supplemental Brief, notifying the Court of certain factual developments since the July 7 hearing. First, Defendants represented that the Commission "no longer intends to use the DOD SAFE system to receive information from the states." Third Decl. of Kris W. Kobach, ECF No. 24-1 ("Third Kobach Decl."), ¶ 1. Instead, Defendants stated that the Director of White House Information Technology was working to "repurpos[e] an existing system that regularly accepts personally identifiable information through a secure, encrypted computer application," and that this new system was expected to be "fully functional by 6:00pm EDT [on July 10, 2017]." *Id.* Second, Defendants provided the Court with a follow-up communication sent to the states, directing election officials to "hold on submitting any data" until this Court resolved Plaintiff's motion for injunctive relief. *Id.*, Ex. A. In light of these developments, Plaintiff moved to further amend the complaint pursuant to Federal Rule of Civil Procedure 15(a)(2), to name as additional defendants the Director of White House Information Technology, the Executive Committee for Presidential Information Technology, and the United States Digital Service, which the Court granted. Pl.'s Mot. to Am. Compl., ECF No. 30; Order, ECF No. 31.

Given the "substantial changes in factual circumstances" since this action was filed, the Court directed Plaintiff to file an amended motion for injunctive relief. Order, ECF No. 31. Plaintiff filed the amended motion on July 13, seeking to enjoin Defendants from "collecting voter roll data from states and state election officials" and to require

Defendants to "disgorge any voter roll data already collected or hereafter received." Proposed Order, ECF No. 35-6, at 1–2. Defendants' response supplied additional information about how the voter roll data would be collected and stored by the "repurposed" White House computer system. *See* Decl. of Charles Christopher Herndon, ECF No. 38-1 ("Herndon Decl."), ¶¶ 3–6. According to Defendants, the new system requires state officials to request an access link, which then allows them to upload data to a "server within the domain electionintergrity.whitehouse.gov." *Id.* ¶ 4. Once the files have been uploaded, "[a]uthorized members of the Commission will be given access" with "dedicated laptops" to access the data through a secure White House network. *Id.* ¶ 4–5. Defendants represent that this process will only require the assistance of "a limited number of technical staff from the White House Office of Administration . . . ." *Id.* ¶ 6. Finally, Defendants represented that the voter roll data uploaded to the SAFE system by the state of Arkansas—the only voter roll information known to the Court that has been transferred in response to the Commission's request—"ha[d] been deleted without ever having been accessed by the Commission." *Id.* ¶ 7.

II. LEGAL STANDARD

Preliminary injunctive relief, whether in the form of temporary restraining order or a preliminary injunction, is "an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011) (quoting *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008)); *see also Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997) ("[A] preliminary injunction is an extraordinary and drastic remedy, one that should not be granted unless the movant, *by a clear showing*, carries the burden of persuasion." (emphasis in original;

quotation marks omitted)). A plaintiff seeking preliminary injunctive relief "must establish [1] that he is likely to succeed on the merits, [2] that he is likely to suffer irreparable harm in the absence of preliminary relief, [3] that the balance of equities tips in his favor, and [4] that an injunction is in the public interest." *Aamer v. Obama*, 742 F.3d 1023, 1038 (D.C. Cir. 2014) (quoting *Sherley*, 644 F.3d at 392 (quoting *Winter*, 555 U.S. at 20) (alteration in original; quotation marks omitted)). When seeking such relief, "'the movant has the burden to show that all four factors, taken together, weigh in favor of the injunction.'" *Abdullah v. Obama*, 753 F.3d 193, 197 (D.C. Cir. 2014) (quoting *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1292 (D.C. Cir. 2009)). "The four factors have typically been evaluated on a 'sliding scale.'" *Davis,* 571 F.3d at 1291 (citation omitted). Under this sliding-scale framework, "[i]f the movant makes an unusually strong showing on one of the factors, then it does not necessarily have to make as strong a showing on another factor." *Id.* at 1291–92.[3]

III. DISCUSSION

A. Article III Standing

As a threshold matter, the Court must determine whether Plaintiff has standing to

[3] The Court notes that it is not clear whether this circuit's sliding-scale approach to assessing the four preliminary injunction factors survives the Supreme Court's decision in *Winter*. *See Save Jobs USA v. U.S. Dep't of Homeland Sec.*, 105 F. Supp. 3d 108, 112 (D.D.C. 2015). Several judges on the United States Court of Appeals for the District of Columbia Circuit ("D.C. Circuit") have "read *Winter* at least to suggest if not to hold 'that a likelihood of success is an independent, free-standing requirement for a preliminary injunction.'" *Sherley*, 644 F.3d at 393 (quoting *Davis*, 571 F.3d at 1296 (concurring opinion)). However, the D.C. Circuit has yet to hold definitively that *Winter* has displaced the sliding-scale analysis. *See id.*; *see also Save Jobs USA*, 105 F. Supp. 3d at 112. In any event, this Court need not resolve the viability of the sliding-scale approach today, as it finds that Plaintiff has failed to show a likelihood of success on the merits and irreparable harm, and that the other preliminary injunction factors are in equipoise.

bring this lawsuit. Standing is an element of this Court's subject-matter jurisdiction under Article III of the Constitution, and requires, in essence, that a plaintiff have "a personal stake in the outcome of the controversy . . . ." *Warth v. Seldin*, 422 U.S. 490, 498 (1975). Consequently, a plaintiff cannot be a mere bystander or interested third-party, or a self-appointed representative of the public interest; he or she must show that defendant's conduct has affected them in a "personal and individual way." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). The familiar requirements of Article III standing are:

> (1) that the plaintiff have suffered an "injury in fact"—an invasion of a judicially cognizable interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) that there be a causal connection between the injury and the conduct complained of—the injury must be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court; and (3) that it be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Bennett v. Spear, 520 U.S. 154, 167 (1997) (citing *Lujan*, 504 U.S. at 560–61). The parties have briefed three theories of standing. Two are based on Plaintiff's own interests—for injuries to its informational interests and programmatic public interest activities—while the third is based on the interests of Plaintiff's advisory board members. This latter theory fails, but the first two succeed, for the reasons detailed below.

1. Associational Standing

An organization may sue to vindicate the interests of its members. To establish this type of "associational" standing, Plaintiff must show that "(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Ass'n of Flight Attendants-CWA, AFL-CIO v. U.S. Dep't of Transp.*, 564 F.3d 462, 464 (D.C. Cir. 2009) (internal

quotation marks omitted). Needless to say, Plaintiff must also show that it has "members" whose interests it is seeking to represent. To the extent Plaintiff does not have a formal membership, it may nonetheless assert organizational standing if "the organization is the functional equivalent of a traditional membership organization." *Fund Democracy, LLC v. S.E.C.*, 278 F.3d 21, 25 (D.C. Cir. 2002). For an organization to meet the test of functional equivalency, "(1) it must serve a specialized segment of the community; (2) it must represent individuals that have all the 'indicia of membership' including (i) electing the entity's leadership, (ii) serving in the entity, and (iii) financing the entity's activities; and (3) its fortunes must be tied closely to those of its constituency." *Washington Legal Found. v. Leavitt*, 477 F. Supp. 2d 202, 208 (D.D.C. 2007) (citing *Fund Democracy*, 278 F.3d at 25).

Plaintiff has submitted the declarations of nine advisory board members from six jurisdictions representing that the disclosure of their personal information—including "name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information"—will cause them immediate and irreparable harm. ECF No. 35-3, Exs. 7–15. The parties disagree on whether these advisory board members meet the test of functional equivalency. For one, Plaintiff's own website concedes that the organization "ha[s] no clients, no customers, and no shareholders . . . ." *See* About EPIC, http://epic.org/epic/about.html (last accessed July 20, 2017). Contrary to this assertion, however, Plaintiff has proffered testimony to the effect that advisory board members exert substantial influence over the affairs of the organization, including by influencing the matters in which the organization participates, and that advisory board members are

expected to contribute to the organization, either financially or by offering their time and expertise. Hr'g Tr. 16:1–18:19; *see also* Decl. of Marc Rotenberg, ECF No. 35-5, Ex. 38, ¶¶ 8–12. In the Court's view, however, the present record evidence is insufficient for Plaintiff to satisfy its burden with respect to associational standing. There is no evidence that members are *required* to finance the activities of the organization; that they have any role in electing the leadership of the organization; or that their fortunes, as opposed to their policy viewpoints, are "closely tied" to the organization. *See id.*; About EPIC, http://epic.org/epic/about.html (last accessed July 20, 2017) ("EPIC *works closely with* a distinguished advisory board, with expertise in law, technology and public policy. . . . EPIC is a 501(c)(3) nonprofit. We have no clients, no customers, and no shareholders. We need your support." (emphasis added)); *see also Elec. Privacy Info. Ctr. v. U.S. Dep't of Educ.*, 48 F. Supp. 3d 1, 22 (D.D.C. 2014) ("defendant raises serious questions about whether EPIC is an association made up of members that may avail itself of the associational standing doctrine").

Furthermore, even if the Court were to find that Plaintiff is functionally equivalent to a membership organization, the individual advisory board members who submitted declarations do not have standing to sue in their own capacities. First, these individuals are registered voters in states that have declined to comply with the Commission's request for voter roll information, and accordingly, they are not under imminent threat of either the statutory or Constitutional harms alleged by Plaintiff. *See* Am. Opp'n Mem., at 13. Second, apart from the alleged violations of the advisory board members' Constitutional privacy rights—the existence of which the Court assumes for purposes of its standing analysis, *see Parker v. D.C.*, 478 F.3d 370, 378 (D.C. Cir. 2007), *aff'd sub nom. D.C. v. Heller*, 554 U.S.

570 (2008)—Plaintiff has failed to proffer a theory of individual harm that is "actual or imminent, [and not merely] conjectural or hypothetical . . . [,]" *Bennett*, 520 U.S. at 167. Plaintiff contends that the disclosure of sensitive voter roll information would cause immeasurable harm that would be "impossible to contain . . . after the fact." Pl.'s Am. Mem., at 13. The organization also alleges that the information may be susceptible to appropriation for unspecified "deviant purposes." *Id.* (internal citations omitted). However, Defendants have represented that they are only collecting voter information that is already publicly available under the laws of the states where the information resides; that they have only requested this information and have not demanded it; and Defendants have clarified that such information, to the extent it is made public, will be de-identified. *See supra* at [•]. All of these representations were made to the Court in sworn declarations, and needless to say, the Court expects that Defendants shall strictly abide by them.

Under these factual circumstances, however, the only practical harm that Plaintiff's advisory board members would suffer, assuming their respective states decide to comply with the Commission's request in the future, is that their already publicly available information would be rendered more easily accessible by virtue of its consolidation on the computer systems that would ultimately receive this information on behalf of the Commission. It may be true, as Plaintiff contends, that there are restrictions on how "publicly available" voter information can be obtained in the ordinary course, such as application and notification procedures. Hr'g Tr. 8:2–21. But even granting the assumption that the Commission has or will receive information in a manner that bypasses these safeguards, the only way that such information would be rendered more accessible for nefarious purposes is if the Court further assumes that either the Commission systems are

more susceptible to compromise than those of the states, or that the de-identification process eventually used by Defendants will not sufficiently anonymize the information when it is publicized. Given the paucity of the record before the Court, this sequence of events is simply too attenuated to confer standing. At most, Plaintiff has shown that its members will suffer an increased *risk* of harm if their already publicly available information is collected by the Commission. But under the binding precedent of the Supreme Court, an increased risk of harm is insufficient to confer standing; rather, the harm must be "certainly impending." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013). Indeed, on this basis, two district courts in this circuit have concluded that even the disclosure of *confidential*, *identifiable* information is insufficient to confer standing until that information is or is about to be used by a third-party to the detriment of the individual whose information is disclosed. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 25 (D.D.C. 2014); *Welborn v. IRS*, 218 F. Supp. 3d 64, 77 (D.D.C. 2016). In sum, the mere increased risk of disclosure stemming from the collection and eventual, anonymized disclosure of already publicly available voter roll information is insufficient to confer standing upon Plaintiff's advisory board members. Consequently, for all of the foregoing reasons, Plaintiff has failed to show that it has associational standing to bring this lawsuit.[4]

[4] This obviates the need to engage in a merits analysis of Plaintiff's alleged Constitutional privacy right claims, which are based on the individual claims of its advisory board members. *See generally* Pl.'s Am. Mem., at 30. Nonetheless, even if the Court were to reach this issue, it would find that Plaintiff is unlikely to succeed on these claims because the D.C. Circuit has expressed "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information." *Am. Fed'n of Gov't Emps., AFL-CIO v. Dep't of Hous. & Urban Dev.*, 118 F.3d 786, 791 (D.C. Cir. 1997).

2. Informational Standing

In order to establish informational standing, Plaintiff must show that "(1) it has been deprived of information that, on its interpretation, a statute requires the government or a third party to disclose to it, and (2) it suffers, by being denied access to that information, the type of harm Congress sought to prevent by requiring disclosure." *Friends of Animals v. Jewell*, 828 F.3d 989, 992 (D.C. Cir. 2016). "[A] plaintiff seeking to demonstrate that it has informational standing generally 'need not allege any additional harm beyond the one Congress has identified.'" *Id.* (citing *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1544 (2016)). Plaintiff has brought suit under the APA, for the failure of one or more federal agencies to comply with Section 208 of the E-Government Act. That provision mandates that before "initiating a new collection of information," an agency must "conduct a privacy impact assessment," "ensure the review of the privacy impact assessment by the Chief Information Officer," and "if practicable, after completion of the review . . . , make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." E-Government Act, § 208(b). An enumerated purpose of the E-Government Act is "[t]o make the Federal Government more transparent and accountable." *Id.* § 2(b)(9).

Plaintiff satisfies both prongs of the test for informational standing. First, it has espoused a view of the law that entitles it to information. Namely, Plaintiff contends that Defendants are engaged in a new collection of information, and that a cause of action is available under the APA to force their compliance with the E-Government Act and to require the disclosure of a Privacy Impact Assessment. Second, Plaintiff contends that it has suffered the very injuries meant to be prevented by the disclosure of information

pursuant to the E-Government Act—lack of transparency and the resulting lack of opportunity to hold the federal government to account. This injury is particular to Plaintiff, given that it is an organization that was "established . . . to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age." About EPIC, https://www.epic.org/epic /about.html (last accessed July 20, 2017). Plaintiff, moreover, engages in government outreach by "speaking before Congress and judicial organizations about emerging privacy and civil liberties issues[,]" *id.*, and uses information it obtains from the government to carry out its mission to educate the public regarding privacy issues, Hr'g Tr. 20:12–23.

Defendants have contested Plaintiff's informational standing, citing principally to the D.C. Circuit's analysis in *Friends of Animals*. *See* Am. Opp'n Mem., at 14–20. There, the court held that plaintiff, an environmental organization, did not have informational standing under a statute that required the Department of the Interior ("DOI"), *first*, to make certain findings regarding whether the listing of a species as endangered is warranted within 12 months of determining that a petition seeking that relief "presents substantial scientific or commercial information," and *second*, after making that finding, to publish certain information in the Federal Register, including under some circumstances, a proposed regulation, or an "evaluation of the reasons and data on which the finding is based." *Friends of Animals*, 828 F.3d at 990–91 (internal quotation marks omitted) (citing 16 U.S.C. § 1533(b)(3)(B)). For example, part of the statute in *Friends of Animals* required that:

> (B) Within 12 months after receiving a petition that is found under subparagraph (A) to present substantial information indicating that the petitioned action may be warranted, the Secretary shall make one of the following findings: . . .
>
> > (ii) The petitioned action is warranted, in which case the Secretary shall promptly publish in the Federal Register a general notice and the complete text of a proposed regulation to implement such action in accordance with paragraph (5).

16 U.S.C. § 1533(b)(3)(B)(ii). At the time plaintiff brought suit, the 12-month period had elapsed, but the DOI had yet to make the necessary findings, and consequently had not published any information in the Federal Register. In assessing plaintiff's informational standing, the D.C. Circuit focused principally on the structure of the statute that allegedly conferred on plaintiff a right to information from the federal government. *Friends of Animals*, 828 F.3d at 993. Solely on that basis, the court determined that plaintiff was not entitled to information because a right to information (e.g., a proposed regulation under subsection (B)(ii) or an evaluation under subsection (B)(iii)) arose only *after* the DOI had made one of the three findings envisioned by the statute. True, the DOI had failed to make the requisite finding within 12 months. But given the statutorily prescribed sequence of events, plaintiff's challenge was in effect to the DOI's failure to make such a finding, rather than to its failure to disclose information, given that the obligation to disclose information only arose after a finding had been made. As such, the D.C. Circuit concluded that plaintiff lacked informational standing.

The statutory structure here, however, is quite different. The relevant portion of Section 208 provides the following:

> (b) PRIVACY IMPACT ASSESSMENTS.—
> (1) RESPONSIBILITIES OF AGENCIES.
> (A) IN GENERAL.—An agency shall take actions described under subparagraph (B) before
> (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
> (ii) initiating a new collection of information that—
> (I) will be collected, maintained, or disseminated using information technology; and
> (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.
> (B) AGENCY ACTIVITIES.—To the extent required under subparagraph (A), each agency shall—
> (i) conduct a privacy impact assessment;
> (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and
> (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

E-Government Act, § 208(b). As this text makes clear, the statutorily prescribed sequence of events here is reversed from the sequence at issue in *Friends of Animals*. There, the DOI was required to disclose information only *after* it had made one of three "warranted" findings; it had not made any finding, and accordingly, was not obligated to disclose any information. Here, the statute mandates that an "agency *shall* take actions described under subparagraph (B) *before* . . . initiating a new collection of information . . . ." *Id.* (emphasis added). Subparagraph (B) in turn requires the agency to conduct a Privacy Impact Assessment, to have it reviewed by the Chief Information Officer or his equivalent, and to publish the assessment, if practicable. The statute, given its construction, requires all three of these events, including the public disclosure of the assessment, to occur *before* the

agency initiates a new collection of information. Assuming that the other facets of Plaintiff's interpretation of the law are correct—namely, that Defendants are engaged in a new collection of information subject to the E-Government Act, that judicial review is available under the APA, and that disclosure of a privacy assessment is "practicable"—then Plaintiff is presently entitled to information pursuant to the E-Government Act, because the disclosure of information was already supposed to have occurred; that is, a Privacy Impact Assessment should have been made publicly available before Defendants systematically began collecting voter roll information. Accordingly, unlike in *Friends of Animals*, a review of the statutory text at issue in this litigation indicates that, under Plaintiff's interpretation of the law, Defendants have already incurred an obligation to disclose information.

Defendants make three further challenges to Plaintiff's informational standing, none of which are meritorious. First, Defendants contend that Plaintiff lacks standing because its informational injury is merely a "generalized grievance," and therefore insufficient to confer standing. Am. Opp'n Mem., at 15 (citing *Judicial Watch, Inc. v. FEC*, 180 F.3d 277, 278 (D.C. Cir. 1999)). Plainly, the E-Government Act entitles the public generally to the disclosure of Privacy Impact Assessments, but that does not mean that the informational injury in this case is not particular to Plaintiff. As already noted, Plaintiff is a public-interest organization that focuses on privacy issues, and uses information gleaned from the government to educate the public regarding privacy, and to petition the government regarding privacy law. *See supra* at [•]. Accordingly, the informational harm in this case, as it relates to Plaintiff, is "concrete and particularized." Moreover, the reality of statutes that confer informational standing is that they are often not targeted at a

particular class of individuals, but rather provide for disclosure to the public writ large. *See, e.g.*, *Friends of Animals*, 824 F.3d at 1041 (finding that public interest environmental organization had standing under statutory provision that required the Department of the Interior to publish certain information in the Federal Register). Even putting aside the particularized nature of the informational harm alleged in this action, however, the fact that a substantial percentage of the public is subject to the same harm does not automatically render that harm inactionable. As the Supreme Court observed in *Akins*: "Often the fact that an interest is abstract and the fact that it is widely shared go hand in hand. But their association is not invariable, and where a harm is concrete, though widely shared, the Court has found 'injury in fact.'" *FEC v. Akins*, 524 U.S. 11, 24 (1998). The Court went on to hold, in language that is particularly apt under the circumstances, that "the informational injury at issue . . . , directly related to voting, the most basic of political rights, is sufficiently concrete and specific . . . ." *Id.* at 24–25.

Defendants next focus on the fact that the information sought does not yet exist in the format in which it needs to be disclosed (i.e., as a Privacy Impact Assessment). Am. Opp'n Mem., at 17. In this vein, they claim that *Friends of Animals* stands for the proposition that the government cannot be required to create information. The Court disagrees with this interpretation of *Friends of Animals*, and moreover, Defendants' view of the law is not evident in the controlling Supreme Court and D.C. Circuit precedents. As already detailed, the court in *Friends of Animals* looked solely to the statutory text to determine whether an obligation to disclose had been incurred. No significance was placed by the D.C. Circuit on the fact that, if there were such an obligation, the federal government would potentially be required to "create" the material to be disclosed (in that case, either a

proposed regulation, or an evaluative report). Furthermore, *Friends of Animals* cited two cases, one by the D.C. Circuit and the other by the Supreme Court, as standing for the proposition that plaintiffs have informational standing to sue under "statutory provisions that guarantee[] a right to receive information *in a particular form*." *Friends of Animals*, 828 F.3d at 994 (emphasis added; citing *Zivotofsky ex rel. Ari Z. v. Sec'y of State*, 444 F.3d 614, 615–19 (D.C. Cir. 2006), and *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373–75 (1982)). Furthermore, in *Public Citizen*, the Supreme Court found that plaintiff had informational standing to sue under FACA, and thereby seek the disclosure of an advisory committee charter and other materials which FACA requires advisory committees to create and make public. Presumably those materials did not exist, given defendants' position that the committee was not subject to FACA, and in any event, the Court made no distinction on this basis. *Pub. Citizen v. U.S. Dep't of Justice*, 491 U.S. 440, 447 (1989). And in *Akins*, the information sought was not in defendants' possession, as the entire lawsuit was premised on requiring defendant to take enforcement action to obtain that information. 524 U.S. at 26. Ultimately, the distinction between information that already exists, and information that needs to be "created," if not specious, strikes the Court as an unworkable legal standard. Information does not exist is some ideal form. When the government discloses information, it must always first be culled, organized, redacted, reviewed, and produced. Sometimes the product of that process, as under the Freedom of Information Act, is a production of documents, perhaps with an attendant privilege log. *See, e.g., Judicial Watch, Inc. v. Food & Drug Admin.*, 449 F.3d 141, 146 (D.C. Cir. 2006) (explaining the purpose of a *Vaughn* index). Here, Congress has mandated that disclosure take the form of a Privacy Impact Assessment, and that is what Plaintiff has standing to

seek, regardless of whether an agency is ultimately required to create the report.

Lastly, Defendants contend that Plaintiff lacks informational standing because Section 208 only requires the publication of a Privacy Impact Statement if doing so is "practicable." Am. Opp'n Mem., at 17 n.2. As an initial matter, Defendants have at no point asserted that it would be impracticable to create and publish a Privacy Impact Assessment; rather, they have rested principally on their contention that they are not required to create or disclose one because Plaintiff either lacks standing, or because the E-Government Act and APA only apply to federal agencies, which are not implicated by the collection of voter roll information. Accordingly, whatever limits the word "practicable" imposes on the disclosure obligations of Section 208, they are not applicable in this case, and therefore do not affect Plaintiff's standing to bring this lawsuit. As a more general matter, however, the Court disagrees with Defendants' view that merely because a right to information is in some way qualified, a plaintiff lacks informational standing to seek vindication of that right. For this proposition, Defendants again cite *Friends of Animals*, contending that the D.C. Circuit held that "informational standing only exists if [the] statute 'guaranteed a right to receive information in a particular form . . . .'" *Id.* (citing *Friends of Animals*, 828 F.3d at 994). That is not what the D.C. Circuit held; rather that language was merely used to describe two other cases, *Haven* and *Zivotofsky*, in which the Supreme Court and D.C. Circuit determined that plaintiffs had informational standing. *See supra* at [•]. One only need to look toward the Freedom of Information Act, under which litigants undoubtedly have informational standing despite the fact that the Act in no way provides an unqualified right to information, given its numerous statutory exemptions. *See Zivotofsky*, 444 F.3d at 618. Moreover, the available guidance indicates that the qualifier "practicable" was meant

to function similarly to the exemptions under the Freedom of Information Act, and is therefore not purely discretionary. *See* M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003) ("Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment. *Such information shall be protected and handled consistent with the Freedom of Information Act* . . . ." (footnote omitted; emphasis added)). Accordingly, for all of the foregoing reasons, the Court concludes that Plaintiff has satisfied its burden at this stage regarding its informational standing to seek the disclosure of a Privacy Impact Assessment pursuant to Section 208 of the E-Government Act.

Moreover, because the Court assumes the merits of Plaintiff's claims for standing purposes, the Court also finds that Plaintiff has informational standing with respect to its FACA claim, which likewise seeks the disclosure of a Privacy Impact Assessment. *Judicial Watch, Inc. v. U.S. Dep't of Commerce*, 583 F.3d 871, 873 (D.C. Cir. 2009) ("Here the injury requirement is obviously met. In the context of a FACA claim, an agency's refusal to disclose information that the act requires be revealed constitutes a sufficient injury.)

3. Organizational Standing Under PETA

For similar reasons to those enumerated above with respect to informational standing, the Court also finds that Plaintiff has organizational standing under *PETA v. USDA*, 797 F.3d 1087 (D.C. Cir. 2015). In this circuit, an organization may establish standing if it has "suffered a concrete and demonstrable injury to its activities, mindful that,

under our precedent, a mere setback to . . . abstract social interests is not sufficient." *Id.* at 1093 (internal quotation marks and alterations omitted) (citing *Am. Legal Found. v. FCC*, 808 F.2d 84, 92 (D.C. Cir. 1987) ("The organization must allege that discrete programmatic concerns are being directly and adversely affected by the defendant's actions."). "Making this determination is a two-part inquiry—we ask, first, whether the agency's action or omission to act injured the organization's interest and, second, whether the organization used its resources to counteract that harm." *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 919 (D.C. Cir. 2015) (internal quotation marks and alterations omitted). In *PETA*, the D.C. Circuit found that an animal rights organization had suffered a "denial of access to bird-related . . . information including, in particular, investigatory information, and a means by which to seek redress for bird abuse . . . ." *PETA*, 797 F.3d at 1095. This constituted a "cognizable injury sufficient to support standing" because the agency's failure to comply with applicable regulations had impaired PETA's ability to bring "violations to the attention of the agency charged with preventing avian cruelty and [to] continue to educate the public." *Id.*

Under the circumstances of this case, Plaintiff satisfies the requirements for organizational standing under *PETA*. Plaintiff has a long-standing mission to educate the public regarding privacy rights, and engages in this process by obtaining information from the government. Pl.'s Reply Mem. at 17 ("EPIC's mission includes, in particular, educating the public about the government's record on voter privacy and promoting safeguards for personal voter data."). Indeed, Plaintiff has filed Freedom of Information Act requests in this jurisdiction seeking the disclosure of the same type of information, Privacy Impact Assessments, that it claims has been denied in this case. *See, e.g.*, *Elec. Privacy Info. Ctr.*

v. DEA, 208 F. Supp. 3d 108, 110 (D.D.C. 2016). Furthermore, Plaintiff's programmatic activities—educating the public regarding privacy matters—have been impaired by Defendants' alleged failure to comply with Section 208 of the E-Government Act, since those activities routinely rely upon access to information from the federal government. *See* Hr'g Tr. at 20:8–16. This injury has required Plaintiff to expend resources by, at minimum, seeking records from the Commission and other federal entities concerning the collection of voter data. *See* Decl. of Eleni Kyriakides, ECF No. 39-1, ¶ 6. Accordingly, Plaintiff has organizational standing under the two-part test sanctioned by the D.C. Circuit in *PETA*.

B. Likelihood of Success on the Merits

Having assured itself of Plaintiff's standing to bring this lawsuit, the Court turns to assess the familiar factors for determining whether a litigant is entitled to preliminary injunctive relief; in this case, a temporary restraining order and preliminary injunction. The first, and perhaps most important factor, is Plaintiff's likelihood of success on the merits.

The E-Government Act does not provide for a private cause of action, and accordingly, Plaintiff has sought judicial review pursuant to Section 702 of the APA. *See Greenspan v. Admin. Office of the United States Courts*, No. 14CV2396 JTM, 2014 WL 6847460, at *8 (N.D. Cal. Dec. 4, 2014). Section 704 of the APA, in turn, limits judicial review to "final agency action for which there is no other adequate remedy . . . ." As relevant here, the reviewing court may "compel agency action unlawfully withheld or unreasonably delayed." 5 U.S.C. § 706(1). The parties principally disagree over whether any "agency" is implicated in this case such that there could be an "agency action" subject to this Court's review. *See* Pl.'s Am. Mem., at 19–30; Am. Opp'n Mem., at 20–33.

"Agency" is broadly defined by the APA to include "each authority of the

Government of the United States, whether or not it is within or subject to review by another agency . . . ." 5 U.S.C. § 551(1). The statute goes on to exclude certain components of the federal government, including Congress and the federal courts, but does not by its express terms exclude the President, or the Executive Office of the President ("EOP"). *Id.* Nonetheless, the Supreme Court has concluded that the President is exempted from the reach of the APA, *Franklin v. Massachusetts*, 505 U.S. 788, 800–01 (1992), and the D.C. Circuit has established a test for determining whether certain bodies within the Executive Office of the President are sufficiently close to the President as to also be excluded from APA review, *see Armstrong v. Exec. Office of the President*, 90 F.3d 553, 558 (D.C. Cir. 1996) (citing *Meyer v. Bush*, 981 F.2d 1288 (D.C. Cir. 1993)). In determining whether the Commission is an "agency," or merely an advisory body to the President that is exempted from APA review, relevant considerations include "whether the entity exercises substantial independent authority," "whether the entity's sole function is to advise and assist the President," "how close operationally the group is to the President," "whether it has a self-contained structure," and "the nature of its delegated authority." *Citizens for Responsibility & Ethics in Washington v. Office of Admin.*, 566 F.3d 219, 222 (D.C. Cir. 2009) ("*CREW*") (internal quotation marks omitted). The most important consideration appears to be whether the "entity in question wielded substantial authority independently of the President." *Id.*

The record presently before the Court is insufficient to demonstrate that the Commission is an "agency" for purposes of the APA. First, the Executive Order indicates that the Commission is purely advisory in nature, and that it shall disband shortly after it delivers a report to the President. No independent authority is imbued upon the

Commission by the Executive Order, and there is no evidence that it has exercised any independent authority that is unrelated to its advisory mission. Defendants' request for information is just that—a request—and there is no evidence that they have sought to turn the request into a demand, or to enforce the request by any means. Furthermore, the request for voter roll information, according to Defendants, is ancillary to the Commission's stated purpose of producing an advisory report for the President regarding voting processes in federal elections. The Executive Order does provide that other federal agencies "shall endeavor to cooperate with the Commission," and that the GSA shall "provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission." Exec. Order § 7(a). Nonetheless, Defendants have represented that the GSA's role is currently expected to be limited to specific "administrative support like arranging travel for the members" of the Commission, and that no other federal agencies are "cooperating" with the Commission. Hr'g Tr. at 27:25–28:6; 30:10–13. Finally, although Commissioner Christy McCormick of the Election Assistance Commission is a member of the Commission, there is currently no record evidence that she was substantially involved in the decision to collect voter information, or that her involvement in some fashion implicated the Election Assistance Commission, which is a federal agency. Hr'g Tr. 28:24–30:4; *cf. Judicial Watch, Inc. v. Nat'l Energy Policy Dev. Grp.*, 219 F. Supp. 2d 20, 39–40 (D.D.C. 2002) (citing *Ryan v. Dep't of Justice*, 617 F.2d 781 (D.C. Cir. 1980)).

This would have ended the inquiry, but for the revelation during the course of these proceedings that the SAFE system, which the Commission had intended for states to use to transmit voter roll information, is operated by a component of the Department of

Defense. Moreover, the only voter roll information transferred to date resided on the SAFE system, and consequently was stored on a computer system operated by the Department of Defense. Given these factual developments, the Department of Defense—a federal agency—was added as a defendant to this lawsuit. *See* Am. Compl., ECF No. 21, ¶¶ 37–42. Shortly after that occurred, however, Defendants changed gears, and represented that "[i]n order not to impact the ability of other customers to use the [SAFE] site, the Commission has decided to use alternative means for transmitting the requested data." ECF No. 24, at 1. In lieu of the SAFE system, Defendants had the Director of White House Information Technology ("DWHIT") repurpose "an existing system that regularly accepts personally identifiable information through a secure, encrypted computer application within the White House Information Technology enterprise." *Id*. Furthermore, Defendants have represented that the data received from the State of Arkansas via the SAFE system has been deleted, "without ever having been accessed by the Commission." Herndon Decl. ¶ 7. Accordingly, while the legal dispute with respect to the use of the SAFE system by Defendants to collect at least some voter roll information may not be moot—data was in fact collected before a Privacy Impact Assessment was conducted pursuant to the E-Government Act—that potential legal violation does not appear to be a basis for the prospective injunctive relief sought by Plaintiff's amended motion for injunctive relief; namely, the prevention of the further collection of voter roll information by the Commission. In any event, Plaintiff has not pursued the conduct of the Department of Defense as a basis for injunctive relief.

Given the change of factual circumstances, the question now becomes whether any of the entities that will be involved in administering the "repurposed" White House system

are "agencies" for purposes of APA review. One candidate is the DWHIT. According to the Presidential Memorandum establishing this position, the "Director of White House Information Technology, on behalf of the President, shall have the primary authority to establish and coordinate the necessary policies and procedures for operating and maintaining the information resources and information systems provided to the President, Vice President, and the EOP." Mem. on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology ("DWHIT Mem."), § 1, *available at* https://www.gpo.gov/fdsys/pkg/DCPD-201500185/pdf/DCPD-201500185.pdf (last accessed July 16, 2017). The DWHIT is part of the White House Office, *id.* § 2(a)(ii), a component of the EOP "whose members assist the President with those tasks incidental to the office." *Alexander v. F.B.I.*, 691 F. Supp. 2d 182, 186 (D.D.C. 2010), *aff'd*, 456 F. App'x 1 (D.C. Cir. 2011); *see also* Herndon Decl. ¶ 1. According to the Memorandum, the DWHIT "shall ensure the effective use of information resources and information systems provided to the President, Vice President, and EOP in order to improve mission performance, and shall have the appropriate authority to promulgate all necessary procedures and rules governing these resources and systems." DWHIT Mem., § 2(c). The DWHIT is also responsible for providing "policy coordination and guidance" for a group of other entities that provide information technology services to the President, Vice President, and the EOP, known as the "Presidential Information Technology Community." *Id.* § 2(a), (c). Furthermore, the DWHIT may "advise and confer with appropriate executive departments and agencies, individuals, and other entities as necessary to perform the Director's duties under this memorandum." *Id.* § 2(d).

Taken as a whole, the responsibilities of the DWHIT based on the present record

amount to providing operational and administrative support services for information technology used by the President, Vice President, and close staff. Furthermore, to the extent there is coordination with other federal agencies, the purpose of that coordination is likewise to ensure the sufficiency and quality of information services provided to the President, Vice President, and their close staff. Given the nature of the DWHIT's responsibilities and its proximity to the President and Vice President, it is not an agency for the reasons specified by the D.C. Circuit in *CREW* with respect to the Office of Administration ("OA"). In that case, the D.C. Circuit held that the OA was not an "agency" under FOIA[5] because "nothing in the record indicate[d] that OA performs or is authorized to perform tasks other than operational and administrative support for the President and his staff . . . ." *CREW*, 566 F.3d at 224. Relying on its prior holding in *Sweetland*, the court held that where an entity within the EOP, like the DWHIT, provides to the President and his staff "only operational and administrative support . . . it lacks the substantial

[5] Plaintiff argues that *CREW* and similar cases by the D.C. Circuit interpreting whether an entity is an agency for purposes of FOIA are not applicable to determining whether an entity is an agency for purposes of the APA. *See* Pl.'s Reply Mem. at 2. The Court disagrees. The D.C. Circuit established the "substantial independent authority" test in *Soucie,* a case that was brought under FOIA, but at a time when the definition of "agency" for FOIA purposes mirrored the APA definition. In that case, the D.C. Circuit held that "the APA apparently confers agency status on any administrative unit with *substantial independent authority* in the exercise of specific functions." *Soucie v. David*, 448 F.2d 1067, 1073 (D.C. Cir. 1971) (emphasis added); *Meyer*, 981 F.2d at 1292 n.1 ("[b]efore the 1974 Amendments, FOIA simply had adopted the APA's definition of agency"); *see also Dong v. Smithsonian Inst.*, 125 F.3d 877, 881 (D.C. Cir. 1997) ("[o]ur cases have followed the same approach, requiring that an entity exercise substantial independent authority before it can be considered an agency for § 551(1) purposes"—that is, the section that defines the term "agency" for purposes of the APA). The *CREW* court applied the "substantial independent authority" test, and the Court sees no basis to hold that the reasoning of *CREW* is not dispositive of DWHIT's agency status in this matter.

independent authority we have required to find an agency covered by FOIA . . . ." *Id.* at 223 (citing *Sweetland v. Walters*, 60 F.3d 852, 854 (D.C. Cir. 1995)). This conclusion was unchanged by the fact that the OA, like the DWHIT here, provides support for other federal agencies to the extent they "work at the White House complex in support of the President and his staff." *Id.* at 224. Put differently, the fact that the DWHIT coordinates the information technology support provided by other agencies for the President, Vice President, and their close staff, does not change the ultimate conclusion that the DWHIT is not "authorized to perform tasks other than operational and administrative support for the President and his staff," which means that the DWHIT "lacks substantial independent authority and is therefore not an agency . . . ." *Id.* However, to the extent that DWHIT's responsibilities expand either formally or organically, as a result of its newfound responsibilities in assisting the Commission, this determination may need to be revisited in the factual context of this case.

The other candidates for "agency action" proposed by Plaintiff fare no better. The Executive Committee for Presidential Information Technology and the U.S. Digital Service, even if they were agencies, "will have no role in th[e] data collection process." Herndon Decl. ¶ 6. According to Defendants, apart from the DWHIT, the only individuals who will be involved in the collection of voter roll information are "a limited number of . . . technical staff from the White House Office of Administration." *Id.* Finally, Plaintiff contends that the entire EOP is a "parent agency," and that as a result, the activities of its components, including those of the DWHIT and the Commission, are subject to APA review. However, this view of the EOP has been expressly rejected by the D.C. Circuit and is at odds with the practical reality that the D.C. Circuit has consistently analyzed the

agency status of EOP components on a component-by-component basis. *United States v. Espy*, 145 F.3d 1369, 1373 (D.C. Cir. 1998) ("it has never been thought that the whole Executive Office of the President could be considered a discrete agency under FOIA"). Accordingly, at the present time and based on the record before the Court, it appears that there is no "agency," as that term is understood for purposes of the APA, that is involved in the collection of voter roll information on behalf of the Commission. Because there is no apparent agency involvement at this time, the Court concludes that APA review is presently unavailable in connection with the collection of voter roll information by the Commission.

The last remaining avenue of potential legal redress is pursuant to FACA. Plaintiff relies on Section 10(b) of FACA as a means to seek the disclosure of a Privacy Impact Assessment, as required under certain circumstances by the E-Government Act. *See* Am. Compl, ECF No. 33, ¶¶ 73–74. That section provides that an advisory committee subject to FACA must make publicly available, unless an exception applies under FOIA, "the records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by [the] advisory committee . . . ." 5 U.S.C. app. 2 § 10(b). The flaw with this final approach, however, is that FACA itself does not require Defendants to produce a Privacy Impact Assessment; only the E-Government Act so mandates, and as concluded above, the Court is not presently empowered to exert judicial review pursuant to the APA with respect to Plaintiff's claims under the E-Government Act, nor can judicial review be sought pursuant to the E-Government Act itself, since it does not provide for a private cause of action. Consequently, for all of the foregoing reasons, none of Plaintiff's avenues of potential legal redress appear

to be viable at the present time, and Plaintiff has not demonstrated a likelihood of success on the merits.

C. Irreparable Harm, Balance of the Equities, and the Public Interest

Given that Plaintiff is essentially limited to pursuing an informational injury, many of its theories of irreparable harm, predicated as they are on injuries to the private interests of its advisory board members, have been rendered moot. *See* Pl.'s Am. Mem., at 34–40. Nonetheless, the non-disclosure of information to which a plaintiff is entitled, under certain circumstances itself constitutes an irreparable harm; specifically, where the information is highly relevant to an ongoing and highly public matter. *See, e.g.*, *Elec. Privacy Info. Ctr. v. Dep't of Justice*, 416 F. Supp. 2d 30, 41 (D.D.C. 2006) ("EPIC will also be precluded, absent a preliminary injunction, from obtaining in a timely fashion information vital to the current and ongoing debate surrounding the legality of the Administration's warrantless surveillance program"); *see also Washington Post v. Dep't of Homeland Sec.*, 459 F. Supp. 2d 61, 75 (D.D.C. 2006) ("Because the urgency with which the plaintiff makes its FOIA request is predicated on a matter of current national debate, due to the impending election, a likelihood for irreparable harm exists if the plaintiff's FOIA request does not receive expedited treatment."). Indeed, the D.C. Circuit has held that "stale information is of little value . . . [,]" *Payne Enters, Inc. v. United States*, 837 F.2d 486, 494 (D.C. Cir. 1988), and that the harm in delaying disclosure is not necessarily redressed even if the information is provided at some later date, *see Byrd v. EPA*, 174 F.3d 239, 244 (D.C. Cir. 1999) ("Byrd's injury, however, resulted from EPA's failure to furnish him with the documents until long after they would have been of any use to him."). Here, however, the Court concludes that Plaintiff is not presently entitled to the information that it seeks, and accordingly, Plaintiff

cannot show that it has suffered an irreparable informational injury. To hold otherwise would mean that whenever a statute provides for potential disclosure, a party claiming entitlement to that information in the midst of a substantial public debate would be entitled to a finding of irreparable informational injury, which cannot be so. *See, e.g., Elec. Privacy Info. Ctr. v. Dep't of Justice*, 15 F. Supp. 3d 32, 45 (D.D.C. 2014) ("surely EPIC's own subjective view of what qualifies as 'timely' processing is not, and cannot be, the standard that governs this Court's evaluation of irreparable harm").

Finally, the equitable and public interest factors are in equipoise. As the Court recently held in a related matter, "[p]lainly, as an equitable and public interest matter, more disclosure, more promptly, is better than less disclosure, less promptly. But this must be balanced against the interest of advisory committees to engage in their work . . . ." *Lawyers' Comm. for Civil Rights Under Law v. Presidential Advisory Comm'n on Election Integrity*, No. CV 17-1354 (CKK), 2017 WL 3028832, at *10 (D.D.C. July 18, 2017). Here, the disclosure of a Privacy Impact Assessment may very well be in the equitable and public interest, but creating a right to such disclosure out of whole cloth, and thereby imposing an informational burden on the Commission where none has been mandated by Congress or any other source of law, is not.

IV. CONCLUSION

For all of the foregoing reasons, Plaintiff's [35] Motion for a Temporary Restraining Order and Preliminary Injunction is **DENIED WITHOUT PREJUDICE**.

An appropriate Order accompanies this Memorandum Opinion.

/s/
COLLEEN KOLLAR-KOTELLY
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 17-1320 (CKK)

ORDER
(July 24, 2017)

For the reasons stated in the accompanying Memorandum Opinion, Plaintiff's [35] Motion for a Temporary Restraining Order and Preliminary Injunction is **DENIED WITHOUT PREJUDICE**.

SO ORDERED.

Dated: July 24, 2017

/s/
COLLEEN KOLLAR-KOTELLY
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*, Defendants.	Civil Action No. 1:17-cv-1320 (CKK)

DECLARATION OF KRIS W. KOBACH

I, Kris W. Kobach, declare as follows:

1. I am the Secretary of State of Kansas, having served in that position since 2011. I am also the Vice-Chair of the Presidential Advisory Commission on Election Integrity (the "Commission"), which the President established on May 11, 2017, pursuant to Executive Order 13799. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine Americans' confidence in the integrity of the federal election process.

2. The information provided in this declaration is based on my personal knowledge and upon information provided to me in my official capacity as Vice-Chair of the Commission.

3. The Commission was established within the Executive Office of the President and is chaired by the Vice President. The membership, not more than fifteen, is appointed by the President. The members of the Commission come from federal, state, and local jurisdictions

across the political spectrum. The Commission, which is solely advisory, is charged with submitting a report to the President containing its findings and recommendations. The duties of the Commission are set forth in Executive Order 13799 (attached as Exhibit 1) and the Commission's Charter (attached as Exhibit 2). Pursuant to the Charter, the records of the Commission and any subcommittees shall be maintained pursuant to the Presidential Records Act of 1978.

4. In furtherance of the Commission's mandate, I directed that identical letters (with different addressees) be sent to the secretaries of state or chief election officers of each of the fifty states and the District of Columbia. The letters solicit the views and recommendations of the secretaries of state and request their assistance in providing to the Commission publicly-available voter roll data to enable the Commission to fully analyze vulnerabilities and issues related to voter registration and voting. Specifically, I asked for the following data, "if publicly available under the laws of your state": full first and last names of registrants; middle names or initials if available; addresses; dates of birth; political party (if recorded); last four digits of social security numbers; voter history (elections voted in) from 2006; active/inactive status; cancelled status; information regarding prior felony convictions; information regarding voter registration in another state; military status; and overseas citizen information. The information requested is similar to the information that states are required to maintain and to make available for public inspection under the National Voter Registration Act (NVRA) and the Help America Vote Act (HAVA). *See, e.g.*, 52 U.S.C. §§ 20507(i), 21083. The letter I sent to the Secretary of State of Alabama, which is representative of all the letters, is attached as Exhibit 3.

5. In these letters, I requested that the states respond by July 14, 2017, and described two methods for responding. I intended that narrative responses, not containing voter roll data,

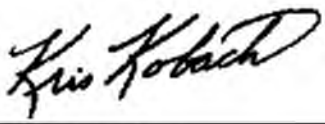
be sent via email to the address provided in the letter. This email is a White House email address (in the Office of the Vice President) and subject to the security protecting all White House communications and networks. For voter roll data, I intended that the states use the Safe Access File Exchange ("SAFE"), which is a secure method of transferring large files up to two gigabytes (GB) in size. SAFE is a tested and reliable method of secure file transfer used routinely by the military for large, unclassified data sets. It also supports encryption by individual users. My letters state that "documents" submitted to the Commission will be made available to the public. That refers only to the narrative responses. With respect to voter roll data, the Commission intends to de-identify any such data prior to any public release of documents. In other words, the voter rolls themselves will not be released to the public by the Commission. The Commission intends to maintain the data on the White House computer system.

6. To my knowledge, as of July 5, 2017, no Secretary of State had yet provided to the Commission any of the information requested in my letter. I have read media reports that numerous states have indicated that they will decline to provide all or some portion of the information, in some cases because individual state law prohibits such transfer of information. However, it is my belief that there are inaccuracies in those media reports with respect to various states.

7. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

***

Executed this 5th day of July 2017.



Kris W. Kobach

EXHIBIT 1

Federal Register
Vol. 82, No. 93
Tuesday, May 16, 2017

Presidential Documents

Title 3—

The President

Executive Order 13799 of May 11, 2017

Establishment of Presidential Advisory Commission on Election Integrity

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to promote fair and honest Federal elections, it is hereby ordered as follows:

Section 1. *Establishment.* The Presidential Advisory Commission on Election Integrity (Commission) is hereby established.

Sec. 2. *Membership.* The Vice President shall chair the Commission, which shall be composed of not more than 15 additional members. The President shall appoint the additional members, who shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience that the President determines to be of value to the Commission. The Vice President may select a Vice Chair of the Commission from among the members appointed by the President.

Sec. 3. *Mission.* The Commission shall, consistent with applicable law, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President that identifies the following:

(a) those laws, rules, policies, activities, strategies, and practices that enhance the American people's confidence in the integrity of the voting processes used in Federal elections;

(b) those laws, rules, policies, activities, strategies, and practices that undermine the American people's confidence in the integrity of the voting processes used in Federal elections; and

(c) those vulnerabilities in voting systems and practices used for Federal elections that could lead to improper voter registrations and improper voting, including fraudulent voter registrations and fraudulent voting.

Sec. 4. *Definitions.* For purposes of this order:

(a) The term "improper voter registration" means any situation where an individual who does not possess the legal right to vote in a jurisdiction is included as an eligible voter on that jurisdiction's voter list, regardless of the state of mind or intent of such individual.

(b) The term "improper voting" means the act of an individual casting a non-provisional ballot in a jurisdiction in which that individual is ineligible to vote, or the act of an individual casting a ballot in multiple jurisdictions, regardless of the state of mind or intent of that individual.

(c) The term "fraudulent voter registration" means any situation where an individual knowingly and intentionally takes steps to add ineligible individuals to voter lists.

(d) The term "fraudulent voting" means the act of casting a non-provisional ballot or multiple ballots with knowledge that casting the ballot or ballots is illegal.

Sec. 5. *Administration.* The Commission shall hold public meetings and engage with Federal, State, and local officials, and election law experts, as necessary, to carry out its mission. The Commission shall be informed by, and shall strive to avoid duplicating, the efforts of existing government entities. The Commission shall have staff to provide support for its functions.

Sec. 6. *Termination*. The Commission shall terminate 30 days after it submits its report to the President.

Sec. 7. *General Provisions*. (a) To the extent permitted by law, and subject to the availability of appropriations, the General Services Administration shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis.

(b) Relevant executive departments and agencies shall endeavor to cooperate with the Commission.

(c) Insofar as the Federal Advisory Committee Act, as amended (5 U.S.C. App.) (the "Act"), may apply to the Commission, any functions of the President under that Act, except for those in section 6 of the Act, shall be performed by the Administrator of General Services.

(d) Members of the Commission shall serve without any additional compensation for their work on the Commission, but shall be allowed travel expenses, including per diem in lieu of subsistence, to the extent permitted by law for persons serving intermittently in the Government service (5 U.S.C. 5701–5707).

(e) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(g) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,
May 11, 2017.

[FR Doc. 2017–10003
Filed 5–15–17; 8:45 am]
Billing code 3295–F7–P

EXHIBIT 2

CHARTER

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY

1. **Committee's Official Designation**. Presidential Advisory Commission on Election Integrity ("Commission").

2. **Authority**. The Commission is established in accordance with Executive Order 13799 of May 11, 2017, "Establishment of a Presidential Advisory Commission on Election Integrity," ("Order") and the provisions of the Federal Advisory Committee Act ("FACA"), as amended (5 U.S.C. App.).

3. **Objectives and Scope of Activities**. The Commission will, consistent with applicable law and the Order, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President of the United States ("President") that identifies the following:

    a. those laws, rules, policies, activities, strategies, and practices that enhance the American people's confidence in the integrity of the voting processes used in Federal elections;
    b. those laws, rules, policies, activities, strategies, and practices that undermine the American people's confidence in the integrity of voting processes used in Federal elections; and
    c. those vulnerabilities in voting systems and practices used for Federal elections that could lead to improper voter registrations and improper voting, including fraudulent voter registrations and fraudulent voting.

4. **Description of Duties**. The Commission will function solely as an advisory body.

5. **Agency or Official to Whom the Committee Reports**. The Commission shall provide its advice and recommendations to the President.

6. **Agency Responsible for Providing Support**. The General Services Administration ("GSA") shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission, to the extent permitted by law and on a reimbursable basis. However, the President's designee will be responsible for fulfilling the requirements of subsection 6(b) of the FACA.

7. **Estimated Annual Operating Costs and Staff Years**. The estimated annual costs to operate the Commission are approximately $250,000 in FY2017 and approximately $250,000 in FY2018, as needed, including approximately three full-time equivalent employees (FTEs) over the duration of the Commission.

8. **Designated Federal Officer**. Pursuant to 41 CFR § 102-3.105 and in consultation with the chair of the Commission, the GSA Administrator shall appoint a full-time or part-time federal employee as the Commission's Designated Federal Officer ("DFO"). The DFO will approve or

call all Commission meetings, prepare or approve all meeting agendas, attend all Commission meetings and any subcommittee meetings, and adjourn any meeting when the DFO determines adjournment to be in the public interest. In the DFO's discretion, the DFO may utilize other Federal employees as support staff to assist the DFO in fulfilling these responsibilities.

9. **Estimated Number and Frequency of Meetings**. Meetings shall occur as frequently as needed, called, and approved by the DFO. It is estimated the Commission will meet five times at a frequency of approximately 30-60 days between meetings, subject to members' schedules and other considerations.

10. **Duration and Termination**. The Commission shall terminate no more than two (2) years from the date of the Executive Order establishing the Commission, unless extended by the President, or thirty (30) days after it presents its final report to the President, whichever occurs first.

11. **Membership and Designation**.

    (a) The Vice President shall chair the Commission, which shall be composed of not more than fifteen (15) additional members.

    (b) Members shall be appointed by the President of the United States and shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience determined by the President to be of value to the Commission. Members of the Commission may include both regular Government Employees and Special Government Employees.

    (c) The Vice President may select a Vice Chair from among those members appointed by the President, who may perform the duties of the chair if so directed by the Vice President. The Vice President may also select an executive director and any additional staff he determines necessary to support the Commission.

    (d) Members of the Commission will serve without additional compensation. Travel expenses will be allowed, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5701-5707), consistent with the availability of funds.

12. **Subcommittees**. The Chair of the Commission, in consultation with the DFO, is authorized to create subcommittees as necessary to support the Commission's work. Subcommittees may not incur costs or expenses without prior written approval of the Chair or the Chair's designee and the DFO. Subcommittees must report directly to the Commission, and must not provide advice or work products directly to the President, or any other official or agency.

13. **Recordkeeping**. The records of the Commission and any subcommittees shall be maintained pursuant to the Presidential Records Act of 1978 and FACA.

14. **Filing Date**. The filing date of this charter is June 23, 2017.

EXHIBIT 3

Presidential Advisory Commission on Election Integrity

June 28, 2017

The Honorable John Merrill
Secretary of State
PO Box 5616
Montgomery, AL 36103-5616

Dear Secretary Merrill,

I serve as the Vice Chair for the Presidential Advisory Commission on Election Integrity ("Commission"), which was formed pursuant to Executive Order 13799 of May 11, 2017. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President of the United States that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine the American people's confidence in the integrity of federal elections processes.

As the Commission begins it work, I invite you to contribute your views and recommendations throughout this process. In particular:

1. What changes, if any, to federal election laws would you recommend to enhance the integrity of federal elections?
2. How can the Commission support state and local election administrators with regard to information technology security and vulnerabilities?
3. What laws, policies, or other issues hinder your ability to ensure the integrity of elections you administer?
4. What evidence or information do you have regarding instances of voter fraud or registration fraud in your state?
5. What convictions for election-related crimes have occurred in your state since the November 2000 federal election?
6. What recommendations do you have for preventing voter intimidation or disenfranchisement?
7. What other issues do you believe the Commission should consider?

In addition, in order for the Commission to fully analyze vulnerabilities and issues related to voter registration and voting, I am requesting that you provide to the Commission the publicly-available voter roll data for Alabama, including, if publicly available under the laws of your state, the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social

security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.

You may submit your responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE"), which is a secure FTP site the federal government uses for transferring large data files. You can access the SAFE site at https://safe.amrdec.army.mil/safe/Welcome.aspx. We would appreciate a response by July 14, 2017. Please be aware that any documents that are submitted to the full Commission will also be made available to the public. If you have any questions, please contact Commission staff at the same email address.

On behalf of my fellow commissioners, I also want to acknowledge your important leadership role in administering the elections within your state and the importance of state-level authority in our federalist system. It is crucial for the Commission to consider your input as it collects data and identifies areas of opportunity to increase the integrity of our election systems.

I look forward to hearing from you and working with you in the months ahead.

Sincerely,

Kris Kobach

Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*, Defendants.	Civil Action No. 1:17-cv-1320 (CKK)

SECOND DECLARATION OF KRIS W. KOBACH

I, Kris W. Kobach, declare as follows:

As described in my declaration of July 5, 2017, I am the Vice Chair of the Presidential Advisory Commission on Election Integrity. I submit this second declaration in response to the Court's order of July 5, 2017, requesting answers to five enumerated questions. I have addressed each question below. The answers are based on my personal knowledge and upon information provided to me in my official capacity as Vice Chair of the Commission.

1. **Who are the current members of the Presidential Advisory Commission on Election Integrity, and what are their affiliations?**

- Vice President Mike Pence, Vice President of the United States, *Chair* (R)
- Secretary Kris Kobach, Secretary of State for Kansas, *Vice Chair* (R)
- Secretary Connie Lawson, Secretary of State of Indiana (R)
- Secretary Bill Gardner, Secretary of State of New Hampshire (D)
- Secretary Matt Dunlap, Secretary of State of Maine (D)
- Ken Blackwell, former Secretary of State of Ohio (R)
- Commissioner Christy McCormick, Election Assistance Commission (R)
- David Dunn, former Arkansas State Representative (D)
- Mark Rhodes, Wood County, West Virginia Clerk (D)
- Hans von Spakovsky, Senior Legal Fellow, Heritage Foundation (R)

2. **If there are no current members who are officials of a federal agency, what is the likelihood that an official of a federal agency will become a member of the Presidential Advisory Commission on Election Integrity in the near future? Identify any likely members who are currently officials of a federal agency.**

Christy McCormick is a member of the Election Assistance Commission (EAC). However, Ms. McCormick is not serving in her official capacity as a member of the EAC; she was selected based upon her experience in election law and administration, including as an employee of the U.S. Department of Justice. The Commission has no legal relationship with the EAC. The President has discretion to appoint additional members to the Commission. To my knowledge, however, no other federal agency officials are currently under consideration for appointment to the Commission.

3. **To what extent has or will the General Services Administration be involved in the collection and storage of data for the Presidential Advisory Commission on Election Integrity?**

At this time, there are no plans for the General Services Administration to collect or store any voter registration or other elections-related data for the Commission.

4. **Who is the current operator of the website https://safe.amrdec.army.mil/safe/Welcome.aspx?**

The U.S. Army Aviation and Missile Research Development and Engineering Center operates that website, which the White House uses for data transfers. *See* https://safe.amrdec.army.mil/safe/About.aspx.

5. **Who is responsible for collecting and storing data received via the website https://safe.amrdec.army.mil/safe/Welcome.aspx? Who will transfer that data to the Presidential Advisory Commission on Election Integrity?**

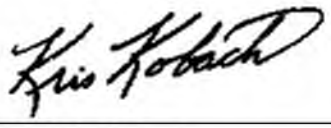
The Safe Access File Exchange (SAFE) is an application for securely exchanging files.

States will upload data to the SAFE website, and Commission staff will download the files from SAFE onto White House computers. As this is a Presidential advisory commission, the White House is responsible for collecting and storing data for the Commission. The Commission's Designated Federal Officer (an employee within the Office of the Vice President) will work with White House Information Technology staff to facilitate collection and storage.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

***

Executed this 6th day of July 2017.



Kris W. Kobach

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

vs. 1:17-cv-1320

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY; MICHAEL PENCE, in his official capacity as Chair of the Presidential Advisory Commission on Election Integrity; KRIS KOBACH, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES; OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES,

Defendants.

TRANSCRIPT OF TEMPORARY RESTRAINING ORDER

BEFORE THE HONORABLE COLLEEN KOLLAR-KOTELLY

UNITED STATES DISTRICT JUDGE

JULY 7, 2017

Court Reporter:
Richard D. Ehrlich, RMR, CRR
Official Court Reporter
United States District Court
333 Constitution Avenue, NW
Washington, DC 20001
(202) 354-3269

Proceedings reported by stenotype.

Transcript produced by computer-aided transcription.

A P P E A R A N C E S

FOR THE PLAINTIFF:

MARC ROTENBERG
ALAN J. BUTLER
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org
butler@epic.org

FOR THE DEFENDANTS:

ELIZABETH J. SHAPIRO
CAROL FEDERIGHI
JOSEPH E. BORSON
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
(202) 514-5302
Elizabeth.Shapiro@usdoj.gov
Carol.Federighi@usdoj.gov
Joseph.Borson@usdoj.gov

THE COURT: Good afternoon, everyone.

All right. Go ahead and call.

THE CLERK: Civil Case 17-1320, *Electronic Privacy Information Center vs. Presidential Advisory Commission On Election Integrity, et al.*

Counsel, would you please come forward and identify yourself for the record?

MR. ROTENBERG: Your Honor, good afternoon. My name is Marc Rotenberg. I am counsel for the Electronic Privacy Information Center. With me is Alan Butler, also counsel for EPIC.

THE COURT: All right. Good afternoon.

MS. SHAPIRO: Good afternoon, Your Honor. I'm Elizabeth Shapiro from the Department of Justice, and with me at counsel's table is Joseph Borson and Carol Federighi, also from the Department of Justice.

THE COURT: All right. Thank you.

All right. I reviewed the motion for the temporary restraining order, the opposition, or reply, a sur-reply, and a very recently sur sur-reply that I just received.

So I have to say that the last document I've received I've looked at very quickly but

have not been able to look at everything, but I did look at some of the exhibits, et cetera.

So, obviously, I will need to take a look at that a little bit more. I've also reviewed the pertinent case law.

I'm going to start by stating my overview of what I consider a framework in very summary forms what I would consider in informing my decision when I make it. I will tell you I'm not making it from the bench today. I do need some information, and that's part of the reason for the hearing.

So I'm going to start with the standing arguments as I understand them in looking at the case law. I'm going to start with informational standing or injury and the general principles that you start by looking at the statute that's at issue that requires a disclosure of information. It would appear from the cases that there would be no informational standing if the statute has a prerequisite to the disclosure of the information. That has not yet happened. There would be no informational injury because the Government has not yet been obligated to disclose the information; however, if you

consider the E-Government Act, which is the statute at issue in this case, it requires that there be a Privacy Impact Assessment and disclosure of that assessment before the, in this case, the election data is collected. So it would appear that it could apply in this particular case.

The Commission moved forward in collecting the electronic -- the election data, rather, where the statute requires an impact statement regarding the collection, and it requires also a disclosure of that impact statement before the collection of the data.

So I think this case fits more into that category when you look at the E-Government Act itself which requires all of this before you start collecting.

So we're talking about -- in this there's been no impact statement done or disclosed prior to collecting the data at issue, which the E-Government Act requires, and the injury here would be the nondisclosure of the impact statement prior to collecting the election data.

In terms of organizational standing, there are at least two theories at issue. One is that

the -- which the plaintiff argues that their members are injured or will be injured if the privacy impact statement is not done. It's not clear to me what harm there would be to the individual members, what they would suffer where the Commission is collecting, according to them, only publicly available information and would only publish in an anonymous form. So I need more information relating to the membership and harm.

Looking at another theory, which is in the PETA case, which is a DC circuit case, the DC circuit recognized a somewhat unique concept of organizational standing; namely, that an organization has standing if it can show, quote, "A concrete and demonstrable injury to its activities mindful that under our precedent a mere setback to abstract social interest is not sufficient."

This would mean that EPIC has standing if it can show that its public interest activities -- I'm assuming educating the public regarding privacy -- will be injured by the defendants' failing to abide by the E-Government Act.

So the injury here, it's argued, would be its public interest activities, educating the public, or whatever, and they would not have the information from the Privacy Impact Assessment prior to the collection of the electronic data.

So the failure would be to provide EPIC important information that they argue vital to its public interest activities. I need more information about this one as well.

So those are, in very summary forms, what I see as the arguments and the framework on which to make a decision on obviously the initial decision which is going to be standing.

Now, I have a series of questions that I'd like to ask, and at the end of all of the questions, I'll give you an opportunity to respond to my overview, to my two views of the informational injury and the organizational.

So I'm going to start with the plaintiff. So why don't you come on up and let me ask a couple of questions here.

So I'm going to start with the members. What concrete harms will EPIC members suffer if their publicly available voter information is collected and publicized by defendants in an

anonymous form?

MR. ROTENBERG: Okay. Thank you, Your Honor. Let me begin by saying that EPIC will take the position that, as a matter of law, none of the information sought by the Commission is, in fact, publicly available to the Commission. I will explain that I believe it is one of the questions you set out in your hearing for today.

The information that is sought from the EPIC members is information that is currently protected under state privacy law. Those state privacy laws limit the collection and use of state voter record information to particular parties and for particular purposes. In our view, the Commission falls outside the bounds of almost all of those exceptions found in the state privacy law for the release of the information that the Commission seeks. That's the basis upon which we say that there is nothing as a matter of law that's publicly available to the Commission given the request in the June 28th letter.

THE COURT: Well, it seemed to me -- and I only got to look at the chart very quickly as one of the exhibits, but it looked as if a

number of states were providing some; a number of states were indicating that they couldn't under their state statutes. There may be some federal statutes relating to Social Security. The Commission has argued that it's only publicly available that they're seeking, and if a state has statutes that would not allow it to produce it, then they are not expecting to get the information.

MR. ROTENBERG: Right. We understand that, Your Honor, and we've attached by way of example the response from the Secretary of State of the State of Georgia, which was similar to the responses from many of the states in which the state secretary says simply much of the information that is sought by the Commission we could not release.

But then you see the state secretary goes on to suggest that there are additional conditions prior to the disclosure. So, for example, the method that has been proposed by the Commission to receive the voter data from the State of Georgia, even that could be permissibly disclosed by the State, the State would not accept, and the State said we would

have to find a different technique, one that is password encrypted and authenticated to permit the release of the personal data; moreover, the State of Georgia also said to the Commission there are fees associated when requests are made for the release of state voter data.

The June 28th letter that was sent to the 50 state secretaries provided no indication that the Commission was prepared to pay any of the fees associated with a release of the data it was seeking.

So you see, there are three different ways to understand how it is that when the Commission approaches the State and asks for so-called publicly available information, the state secretary properly responds under the terms of this letter, "There's, in fact, nothing we can provide to you."

THE COURT: So your idea would be that if they had done an impact -- Privacy Impact Assessment, they would've figured this all out?

MR. ROTENBERG: Well, Your Honor, that's the second category of our objection to the Commission's request. Not only do we believe that the states could not release the

information to the Commission, we further believe that the Commission could not receive the information from the states, and this has to do with the obligations that fall on the Commission by virtue of being within the Executive Office of the President and subject to the Federal Advisory Committee Act and the E-Government Act to undertake certain steps before it could request any type of personal data. It was expected to undertake the Privacy Impact Assessment, which may very well have revealed that the method of transmission proposed in this instance was simply inadequate.

So you see, in requesting the so-called publicly available information, the Commission actually committed two flaws. In the first instance, it did not comply with the requests of the 50 states.

In the second instance, it did not fulfill its own obligations to safeguard the information it was intending to collect.

THE COURT: Okay. But let's get -- that one gets a little bit more to the merits it seems to me.

MR. ROTENBERG: Yes.

THE COURT: Let me get back to sort of the standing question. I appreciate the information.

What concrete harms -- I'm talking about this is -- the EPIC members would suffer if -- assuming that there is any publicly available voter information that can actually be collected. I believe that they've indicated -- I mean, if they're not publicly available, they're not going to receive it, and you've indicated that -- I don't know whether anybody has actually sent anything or whether any of the states can say that they can send it. They're meeting all of the requirements. Do you know?

MR. ROTENBERG: Well, let me say based on the declaration of Mr. Kobach on July 5th, two days ago, the Commission had not received any data from any of the states.

So, at this moment, we're relying on that declaration as to the current status regarding the transfer of the data that's being sought.

But to your question, Your Honor, let's understand two different types of information that the State is seeking. So by the terms of the letter, they ask, for example, for the last

four digits of the Social Security number. Members of EPIC's voter information may well contain the Social Security number. It is often used in the state administration of election systems to avoid duplication and reduce the risk of fraud, but it is not the case that information is generally made available to the public. If it were made available to the public, the last four digits of the Social Security number have been identified by the Department of Justice and consumer protection agencies as contributing to the commission of identity theft and financial fraud because those last four digits are the default passwords for many commercial services such as cell phone or online banking.

So you see, the Commission has asked the states to turn over particular personal information the states would not routinely make available concerning EPIC members that if it were made public could lead to identity theft.

THE COURT: But that assumes -- I think they've indicated, however, that publicly available -- they've left it to the states to figure out, or whatever statutes. So if there's

a federal statute or some other way that they should not be giving out Social Security numbers, or the last four digits of Social Security numbers, the expectation would be that the states would not provide it.

MR. ROTENBERG: I understand your point, Your Honor, but I would add also, I frankly find it striking that a commission on election integrity would make such a broad request to the states for such detailed personal information and then put it back on the states to determine which information the states may lawfully release.

Let me take a simple category. Home addresses. So there is agreement, for example, in the report of the National Conference of State Legislatures, the 2016 report which we've appended to our filing, that surveys the privacy laws of all 50 states. And it says, 29 states, as a general matter, will give out home address -- name and address, I should say precisely, name and address information.

And you could well say, "Well, that appears to be publicly available information. Why can't they just, you know, send back the name and

address information?"

And then you read more closely, and you see that, in fact, even though that information may be made available, many people in the states also have the right to restrict the disclosure of name and address information.

Texas, in fact, restricts the disclosure of the name and address information from the judiciary.

So none of these categories lend themselves to an easy release of state data.

THE COURT: Well, it sounds as if there's not going to be any basis for them to get anything. So your request to hold it back, if they're not going to give it, doesn't seem to work.

I'm still trying to get in terms -- what are the EPIC -- let me ask it this way: Who do you consider the EPIC members? Their advisory board. What does the advisory board do? I mean, the members that you're talking about, the ones you attached were advisory board members and also voters. So what are the rights and responsibilities of EPIC's advisory board members?

MR. ROTENBERG: Okay. So we have approximately 100 members of our advisory board. They are leading experts in law, technology, and public policy that contribute to the support of the organization. They participate in the work of the organization. They help select award recipients for the organization.

THE COURT: Do they pay any kind of dues?

MR. ROTENBERG: There is no formal dues requirement, but most of the members do contribute in some manner to the work of the organization. And in this particular matter, 30 of our 100 members signed a statement to the National Association of Secretaries of State asking state officials not to release the voter data to the Commission.

So we are, in effect, also representing their interest when we appear before --

THE COURT: Who is their interest?

MR. ROTENBERG: I'm sorry?

THE COURT: Who is their interest?

MR. ROTENBERG: Those members of our advisory board who are actively participating and expressing their opposition to the data collection.

THE COURT: Okay. Do they control the activities of the organization?

MR. ROTENBERG: They do not directly control the activities of the organization. There is a separate board of directors, but it is not uncommon for an organization such as EPIC to have this structure, and the members of the advisory board actively participate in the program activities and the direction and selection of matters that the organization pursues.

THE COURT: So exactly what -- the board of directors runs the organization?

MR. ROTENBERG: Yes, that's correct.

THE COURT: And the advisory board advises on what matters to get involved with?

MR. ROTENBERG: Yes, Your Honor, and actively participates in those activities and provides financial support.

THE COURT: But it's a voluntary financial support?

MR. ROTENBERG: That's correct. But they could not -- to be clear on this point, they could not be a member of the advisory board unless they formally accepted that

responsibility, and they may choose to withdraw their participation as an advisory board member as well.

THE COURT: Accepted what responsibility?

MR. ROTENBERG: Participating in the work of the organization.

THE COURT: Okay.

MR. ROTENBERG: Contributing to its activities.

THE COURT: And the contribution you're talking about is contributing in terms of if you decide to take on a particular task such as this one, this particular case, that they would contribute to providing information, pursuing it? Is that what you're saying?

MR. ROTENBERG: Financial support including personal donations are routinely made by members of the advisory board, their time and their expertise.

THE COURT: All right. So what informational harms will EPIC suffer if the defendants don't comply with the E-Government Act, which requires disclosure of this Privacy Impact Assessment to be done and then disclosed before the collection of the data?

Again, I'm talking about EPIC in the context of either membership or otherwise.

MR. ROTENBERG: Right. Well, apart from the individual harm to our members, also as an organization that was specifically established to focus public attention on emerging privacy issues, and has been involved in the voter privacy matter for almost 20 years, this particular controversy directly impacts our mission. This is not a speculative type of arrangement. This is a circumstance where we have for many years sought to advance an interest in voter privacy here in the United States. The actions by the Commission have required us to undertake a number of activities to work with citizen organizations, to discuss with media outlets the impact of the Commission's activity upon the public. That is an educational function which we would not be doing at this point to the extent that we are but for the Commission's request to gather state voter record information.

THE COURT: So as you've described it, I take it that's what you would consider your public interest activities?

MR. ROTENBERG: Well, yes. I mean, there is, in fact, also related litigation. We are seeking under the Open Government Act to obtain information about the Commission's activity. That is also activity undertaken, a cost to the organization, and in response to the Commission's act.

THE COURT: All right. And in terms of educating the public regarding data privacy or other activities, do you use routinely information from the Government?

MR. ROTENBERG: Yes, we do, and I should point out also central to our educational activity is the maintenance of one of the most popular websites in the world on privacy issues, which is simply EPIC.org. So for the last week, as a consequence of the Commission's act, we put aside the other work on our website and focused solely on providing public information related to this current controversy.

So there are two pages of EPIC.org with extensive information about the Commission as well as this litigation.

THE COURT: You started off the discussion by indicating all of the difficulties and

barriers there would be to provide -- having the states provide the voter registration data to the Commission based on various statutes, regulations, or whatever. I take it you're really getting to the merits that this is not publicly available for the most part? Is that the point of this --

MR. ROTENBERG: Correct, Your Honor. And we thought it was important to state that at the outset. We understood in the questions that you had posed to the parties for today's hearing, and certainly Mr. Kobach in his letter to the state secretaries, uses this phrase, "publicly available." He places a great deal of weight on it. But, in fact, we could not find the phrase in any of the state voter privacy laws that we looked at. The states talk about public records in some instances, or they talk about exemptions which permit the release of voter record information. But we thought it was very important to make clear that this phrase is actually not a phrase that helps us understand the permissible circumstances under which the data may be released.

THE COURT: Okay. All right. I have some

questions for the defendant. I'll get back to you.

MR. ROTENBERG: Okay. Thank you.

THE COURT: So my first question is: What's the authority, if any, relied on by the Commission to systematically collect this voter registration information?

I didn't see anything in the materials establishing or anything else that talked about it.

MS. SHAPIRO: Well, I think the main authority is the executive order which sets out the mission of the Commission and the charter based on the executive order. And in order to carry out the work that is defined in those documents, the Commission needs to collect and analyze information so that it can best advise the president in the report that it's charged with creating.

THE COURT: But you would agree that there's nothing in the executive order that suggests that you -- that this data should be collected?

MS. SHAPIRO: There's nothing specific about that, but I don't believe that authority

would be required because it's not a demand for information. It's a request, and the Commission is not empowered to enforce that. It doesn't have the ability to say you must do it. So it's simply a request to the states and nothing more than that.

THE COURT: Do you want to respond to the issue in terms of what he brought up initially relating to the fact that, as it appears that most states, if not all of them, have restrictions, and that there's really nothing that's totally publicly available about the request?

MS. SHAPIRO: So I think if I'm understanding correctly, I think what EPIC is saying is that they don't have standing because the way I understand what they're saying is that the states are not going to provide the information because the information is protected under state law, in which case there won't be information going to the Commission. So there can't possibly be any injury because if the information is not going to the Commission, there's no injury. There's no Article III standing.

THE COURT: Are you talking about in the context of the EPIC injury to EPIC members? Is that what you're talking about?

MS. SHAPIRO: EPIC members.

I also wanted to address the alleged organizational injury because I think that they fail standing on numerous levels. Not only do the members not have standing because their states are not providing the information, but, organizationally, everything that EPIC just discussed now relates to its advocacy mission. And I think the cases are quite clear that simply choosing where to allocate resources when advocating --

THE COURT: But that's only one piece of what he talked about. I mean, if you look at the PETA case, it certainly is -- the argument would be its public interest activities, which in this case is educating the public is that by not having the information relating to the assessment, the impact assessment, they're not in a position to put that information out.

So, I mean -- leaving aside allocating different things. The questions I asked really related to what was the role of the members in

order to make a decision as to whether, you know, the first theory of organizational standing based on membership as opposed to the PETA case, which I think is premised on activities, not on membership.

MS. SHAPIRO: Correct. Though the PETA case identified a concrete injury to the organization, a perceptible injury they called it, because they were not -- in that case, there was agency -- some agency inaction that prevented the organization from filing complaints with the agency. So there was a perceptible injury to the organization.

Here you have an organization whose mission is advocacy. They may be very, very interested in privacy, and they may be expert --

THE COURT: Advocacy but also in terms of informing the public, if I understood. The educational aspect would be informing the public of this information, and they're not getting it.

MS. SHAPIRO: Correct, but the information doesn't exist, and I guess that goes to the informational standing because I believe that the cases require that the information actually be in existence in order to --

THE COURT: You have to look at the statute first. And if you look at the statute, the E-Government Act requires that before the collection of the data take place, that you would've done this impact statement, which is different than the cases that have indicated where the statute requires. What I said is that the prerequisite to the disclosure hadn't happened in the other case, which I think is -- I can't remember which case it is.

MS. SHAPIRO: It was Friends of Animals, I think.

THE COURT: Yeah, in terms of that one, which is not what we're talking about.

E-Government Act doesn't require -- it requires it up front before you would've collected data.

MS. SHAPIRO: Yes. But I think, then, it's a question of the Commission not being subject to the E-Government. So it has no requirement to create that --

THE COURT: That's why we're getting back to some of these standing things.

MS. SHAPIRO: Right.

THE COURT: So let's get back to some of

the other questions that I had.

So your view of it is it's implicit in the executive order that they can collect whatever they think is important for their mission?

MS. SHAPIRO: Right. And I would refer back to the Mayer case, which was the Reagan Task Force on Deregulation that was addressed in *Mayer v. Bush*, a similar kind of commission chaired by the vice president also gathering information in order to make recommendations.

It's not uncommon to think that in the ordinary task of preparing a report and studying an issue, that you would need information.

THE COURT: Okay. I just was curious as to whether there was something I had missed.

What services have or will be provided by GSA to the Commission? Because I notice that the executive order says that, "GSA shall provide the Commission with administrative services, funds, facilities, staff, equipment, other support services as be necessary."

So have they -- is the Commission fully operational? Have they set up an office? Where is it located? Are you using any GSA services?

MS. SHAPIRO: So the Commission is in its

infancy. There has not yet been a meeting. GSA is tasked with specific limited administrative support, like arranging travel for the members, maybe assistance with booking meeting locations. Mostly logistical. That's what's envisioned at this stage.

THE COURT: Okay. Is that what you're expecting it to do in the future?

MS. SHAPIRO: Yes. Of course, the Commission is not really up and running, you know, to any great extent.

THE COURT: Where is it located at this point? Does it have an office?

MS. SHAPIRO: Well, I don't know that it has dedicated office space. I believe it's the Office of the Vice President, since the vice president is the chair of the Committee.

THE COURT: All right. What has been or will be the involvement of Commissioner Christy McCormick and/or the Election Assistance Commission in the decision-making process of the Commission since she heads the Election Assistance Commission?

MS. SHAPIRO: She's a member of the Commission but not there as part of her EAC

role. It's completely distinct from that. She's there as just a member of the Commission due to her expertise, and she would participate in the decision-making and the deliberations to the extent she's present at the meetings.

THE COURT: So there's not going to be any role or any information provided or any role by Election Assistance Commission? Is that what you're saying?

MS. SHAPIRO: Well, she would not be there as part of -- in her capacity -- in that capacity as --

THE COURT: Well, that's not quite what I asked.

MS. SHAPIRO: Okay.

THE COURT: What I asked is -- she's maybe not as the head assigned to it like the state secretary of a particular state, but my question is whether the Election Assistance Commission is going to provide assistance to the Commission?

So you have her -- I mean, there's cases that talk about dual role of being in sort of a private in the government.

MS. SHAPIRO: Right. I'm not aware that they would be providing any assistance. I can

double-check that for the Court, but my understanding is that they would not be providing assistance, and she is on the board simply as a member of the Commission.

THE COURT: All right. The executive order talks about other federal agencies will, quote, "Cooperate with the Commission."

Any other federal agencies currently cooperating with the Commission?

MS. SHAPIRO: No. Right now there are no other federal members of the Commission. I don't know of any other federal agencies working with the Commission.

THE COURT: So let me move into the website in terms of which -- it appears to be an Army website?

MS. SHAPIRO: Yes.

THE COURT: So that's not going to be -- that doesn't involve a federal agency?

MS. SHAPIRO: Well, it's a site that exists to transfer large data sites, but that is more of an IT tool. It's not -- it doesn't involve their -- the military is not engaged in the work of the Commission in any substantive way.

THE COURT: Let me ask it this way. Who

operates the website that's named in the Commission's request? Is that a component of -- it looks -- they did an impact statement themselves about the website, the DOD did, which is obviously a federal agency, or will be considered under the definition.

So who is going to actually operate the website? Somebody has to. I assume it's not the Commission. Is it the DOD?

MS. SHAPIRO: So the way I understand it works is that the user uploads the data, and then it's downloaded by the Commission; that DOD doesn't play a role in that other than maintaining the site. They don't store the data. They don't archive the data. It deletes after two weeks I believe is the maximum amount of time.

THE COURT: So say this again. They maintain it?

MS. SHAPIRO: Well, it's their site.

THE COURT: Right. So they receive the data and maintain it for the two weeks?

MS. SHAPIRO: Well, the person uploading the data can set the time that --

THE COURT: And who is uploading the data?

MS. SHAPIRO: The states, for example. If they want to upload the data to the site, they can set an expiration date of -- it must be less than two weeks. So a maximum of two weeks that it can remain on the server.

THE COURT: So DOD, according to you, has no role?

MS. SHAPIRO: That's right, other than, of course, that it runs the SAFE system.

I did want to address, since we're talking about that system, the declaration that the plaintiff put in about getting insecure or error messages. If you read through the website for SAFE itself, it's clear that it's tested and certified to work with Windows XP and Microsoft Explorer. So the browsers that EPIC's declarant used were Google and Netscape, I believe, not Explorer. If you plug it into Explorer, it works just fine. And that's in two different places on the website where it makes that clear, that that's the browser that you need to use.

I have actually compiled some of the pertinent information from the SAFE site that I can provide to the Court and a copy for the plaintiff as well, if it's helpful.

THE COURT: Certainly.

So let me see if I understand it. The computer system that's going to operate in terms of this information, you seem to be saying that the website by DOD is sort of like a conduit, shall we say --

MS. SHAPIRO: Yes.

THE COURT: -- to a system of your own.

So you're going to have your own database at the Commission?

MS. SHAPIRO: So I don't know exactly what the Commission -- it will be stored in the White House email, or the White House servers. So it will be on the White House system. But what the Commission is going to do by way of using the data and compiling the data, I can't speak to that yet.

THE COURT: So you're assume it's either going to be the Commission or the White House that would own and operate the computer system on which the data is going to be stored?

MS. SHAPIRO: Yes. And the email address that was provided in the letter to the states is a White House email address that's maintained by the White House, the same system that supports

the president and the vice president and secures their communications.

THE COURT: So it gets on the DOD. Then how is it going to be transferred to the White House computer system? Who is doing that?

MS. SHAPIRO: So my understanding is that the Commission then downloads the information from SAFE, and then it would be kept in the White House systems.

THE COURT: So they have an IT staff that's expected to do this?

MS. SHAPIRO: Well, I don't know how they're using or going to use IT staff, but the Office of Administration, which serves the Office of the President generally is also within the Executive Office of the President and maintains the White House systems.

THE COURT: You also -- I believe it was a letter that gave an email address. Who owns and operates the computer system associated with the email?

MS. SHAPIRO: So that's the White House -- the ovp.gov address.

THE COURT: So this will be on the White House --

MS. SHAPIRO: Yeah.

THE COURT: And so any other agencies, federal agencies provide support services for the White House's computer system?

MS. SHAPIRO: Well, I think that's a complicated question simply because some of the details about how the -- the mechanics of the White House IT is something that may not be appropriate to say in a public setting because --

THE COURT: Well, let me just put it this way. Obviously, I'm trying to see if you're getting any -- your argument is E-Government Act doesn't apply because there's no federal agency that's involved.

MS. SHAPIRO: Yes.

THE COURT: So I'm exploring whether there actually is a federal agency that's involved.

MS. SHAPIRO: I understand, but I think the test is not necessarily to look to see if there's one member or one little piece of support.

THE COURT: No. I'm just trying to see in terms of how the data would be -- would come, be collected, stored, whether you're doing a

separate database or how you're doing this. You seem to be indicating that DOD's website would maintain it at least for the period of time until it got transferred, right?

MS. SHAPIRO: Yes. This conduit system would have it for -- until it's downloaded. So from the time it's uploaded until the time it's downloaded for a maximum of two weeks and shorter if that's what's set by the states.

THE COURT: And then you also talked about at some point, although it would be allegedly anonymous, but what system is going to be used to publish the voter information?

MS. SHAPIRO: Well, one publication I think is unclear at this point because it's not clear what would be published. I think Mr. Kobach made clear that the raw data would not be published. That's just -- we don't know at this point.

THE COURT: So do you know who would be making it anonymous? Who would be involved in doing this?

I guess the other question is: Is the White House server in a position to take -- I mean, this is a lot of information. Assuming

all these states actually provided you the information, are they going to actually handle it?

MS. SHAPIRO: I assume --

THE COURT: I could see DOD handling it, but do you know?

MS. SHAPIRO: I don't know, but I'm assuming they have a way to handle it.

THE COURT: All right. I guess I'll start with you and then work back to EPIC, but this is sort of your best arguments on irreparable harm.

How are the defendants harmed if they're required to conduct and disclose a privacy assessment before collecting voter information? Is there any harm to you to do this before you had collected it?

MS. SHAPIRO: Well, yes. I mean, because -- our position is that they're not subject to the E-Government Act because they're not an agency, then we would be required to do something that we're not required to do. So I think there's inherent harm there.

And, you know, there's also a certain amount of -- you know, the privacy assessment is normally done by specific officers and agencies.

So it's set up in a way that doesn't fit very well to the Commission. It talks about chief information officers and positions that are appointed as part of the E-Government Act in agencies. But because the Commission is not an agency, it doesn't have those things. So there would be a certain amount of figuring out what to do with that.

THE COURT: Well, I was provided -- I didn't get a chance to look at all of the exhibits, but it looks as if the Government, or DOD, has already done a -- pursuant to the E-Gov Act -- a privacy impact statement for the website issued by DOD that you plan on having all of this data at least be maintained initially?

MS. SHAPIRO: We got the exhibits 30 minutes before we came here. So I haven't studied them, but that's what it appears to be. But DOD is an agency but the Commission is not.

THE COURT: Okay. And any public interest in foregoing this privacy assessment?

MS. SHAPIRO: I'm sorry. Public interest?

THE COURT: Any public interest? I mean, it's one of the things you have to weigh.

What's your public interest in not doing it?

MS. SHAPIRO: Well, I think --

THE COURT: This is around doing a privacy assessment.

MS. SHAPIRO: I understand.

I think initially plaintiff is seeking extraordinary emergency relief. So, really, the burden is on them, but I think --

THE COURT: I'm going to ask them the same thing, but I'm just asking you. I mean, balancing public interest, is there anything in your perspective?

MS. SHAPIRO: I mean, I think the public interest is that there's, you know, been a priority that there's important work to be done by this commission, and that it should be permitted to go forward, and, you know, do the mission that the president thinks is important to have done. That's in the public interest, to be able to carry on that work.

So, you know, I think there's a public interest in proceeding versus we believe no public interest in the contrary because there's no standing and because there's not an agency involved that's required.

THE COURT: Then, obviously, I have to find standing before we got to this issue.

MS. SHAPIRO: Yes.

THE COURT: I just wanted to see what your answer would be.

Okay. Thank you.

MS. SHAPIRO: I wanted to say one more thing before I forgot.

THE COURT: Certainly.

MS. SHAPIRO: When Mr. Kobach filed his declaration, his first declaration I think on July 5th, we said that no information had come into the site. But yesterday the State of Arkansas did transmit information, and it has not been downloaded. So it hasn't been accessed, but it is in the SAFE site.

THE COURT: So it's on the DOD site?

MS. SHAPIRO: Yes.

THE COURT: That you called a SAFE site.

MS. SHAPIRO: Yes.

THE COURT: Okay.

MS. SHAPIRO: Would Your Honor want a copy?

THE COURT: Yes. If you pass it up to Ms. Patterson, I'd appreciate it, and give it to plaintiffs.

MS. SHAPIRO: Your Honor, I have one more handout, if Your Honor wants it, that relates to standing. It's simply a copy of a decision from 2014, from Judge Amy Berman Jackson that involves EPIC. It's called *EPIC vs. Department of Education*, and it addresses the organizational standing really in very closely analogous circumstances.

THE COURT: Yeah. I'm familiar with the case. I know what it is.

MS. SHAPIRO: I know you are. Okay.

THE COURT: Thank you.

But let me just ask one last question. Since DOD is maintaining -- their website is maintaining the data, why shouldn't they do the assessment? They're a federal agency, and they're basically involved in at least maintaining of the data that's being collected. So why shouldn't they, as a federal agency, do an impact statement relating to the data that they have on their website?

MS. SHAPIRO: So I understand that they've done an assessment for the site, and it can't --

THE COURT: But for the site in general.

MS. SHAPIRO: Right. But it can't be the

case that when you have a sharing site like this, it acts as a conduit, that every time information is uploaded, that you have to have a separate Privacy Impact Assessment.

THE COURT: I don't know that that's necessarily true. I mean, it seems to me -- I'll have to go back and look at the E-Gov Act, but it seems to me if you were dealing with issues of data and privacy, certainly election registration data may be different than some other data in terms of what it would -- what would be done, why they wouldn't be obliged to do one.

MS. SHAPIRO: Because there are very specific requirements. Even in the E-Government Act, they have to be collecting the information. And I think when they are passive --

THE COURT: Well, aren't they collecting it?

MS. SHAPIRO: Well, no, because they're a passive website that -- I mean, a passive site that people upload the information to. You know, DOD is not monitoring what information is being uploaded. It is a way to be able to send large data sets.

THE COURT: But that's true of anything that they use this website for, but they went ahead and did one.

MS. SHAPIRO: They did one for the system.

THE COURT: Right. But, obviously, they thought that it was appropriate to do it. I don't understand the distinction.

MS. SHAPIRO: So I think the distinction is to do it for the security of the site. Writ large is one thing, but to do it every time a user anywhere in the country happens to upload information into it, I don't think it's either required or would be rational.

THE COURT: Well, it may depend on what the information is that's, you know, that's being collected and maintained on the website.

MS. SHAPIRO: I don't think DOD would even know that.

THE COURT: I mean, it may be that they would say their impact statement says there isn't anything further to be said. It's safe as we said before. But I'm just saying, I don't understand why you wouldn't do it if the information is of this type of nature, the nature of this voting registration information.

MS. SHAPIRO: DOD is not monitoring the substance of the information that's coming in. They're not going to know people are uploading different data sets.

THE COURT: Well, it does make a difference. The information is going to sit there. Certainly people could potentially have access to it. It could be hacked or whatever else. Why would you not -- why would they not be required to do one?

MS. SHAPIRO: I think for the reason that the operation of the system, one doesn't fit within the definition of when they're required to do one because they're not collecting as the passive site, but also the practicality of any time somebody uploads information to that site, be it for a day or for the maximum of two weeks, DOD is not monitoring that. They don't know that. They don't know what's in the data. It's a secure passageway.

So the idea --

THE COURT: So are you relying on the E-Gov Act to say that they would not need to do it based on their role in this particular case? I'm trying to figure out what you're relying on.

MS. SHAPIRO: Well, I think that's part of it, yes. So we haven't -- that issue was not before us, so we haven't fully analyzed the requirements of the E-Government Act as applied to DOD, but it does require some active collection.

THE COURT: Okay. All right.

MS. SHAPIRO: Thank you.

THE COURT: Thank you.

MR. ROTENBERG: Your Honor, if I may. I think I have the precise answer to the question you just posed to counsel.

THE COURT: All right.

MR. ROTENBERG: We attached in our supplementary motion this afternoon Exhibit 5, which is, in fact, the Privacy Impact Assessment for the SAFE system, and the very first question asks regarding who the information will be received from. The first box, which is "yes" --

THE COURT: Hold on one second. This is the very last one you put in the file, right?

MR. ROTENBERG: Yes. This is the Notice of Filing of Supplemental Exhibits --

THE COURT: Okay.

MR. ROTENBERG: -- relevant to the

questions raised in the Court's order.

THE COURT: I'm sorry. And you're looking at -- which exhibit number is it?

MR. ROTENBERG: We're looking at Exhibit 5, the very first page.

THE COURT: Okay. I see it.

MR. ROTENBERG: And do you see, there are different scenarios. In fact, the DOD is very much aware of who makes use of the website. The first option refers to receiving information from members of the general public. That box is not checked. It's the subsequent box which says from federal personnel and/or federal contractors. That box is checked. And state secretaries would not qualify on that basis.

Moreover, if I may point out, these are pages 32 and 33 in the ECF, the PIA sets out a fairly narrow set of circumstances under which it may be used for the transfer of official information. And as to the question do individuals have the opportunities to object, the basis of saying "yes" is by not sending personally identifiable information through the transfer system.

So we would say by the terms of the

agencies' own Privacy Impact Assessment, it is not suitable for the purpose that the Commission proposes.

But if I may make one other point that is also relevant to this. We actually don't believe that the Commission had the authority to turn to the military agency to receive the information because if you look at both the executive order and the Commission's charter, it is the GAO that is described as providing not only administrative services but also --

THE COURT: GAO or GSA?

MR. ROTENBERG: GSA. Thank you.

It is the GSA that provides not simply administrative services, this is not just, you know, arranging travel plans, this is also facilities and equipment. Those words appear in the president's executive order. And in the charter implementing the work of the Commission, paragraph 6 describes, quote, "The agency responsible for providing support."

And in that paragraph, these terms "administrative services, facilities, and equipment" appear as well.

So it's entirely unclear to us upon what

legal basis the vice chair had to direct the state secretaries of state to send this information to the proposed military website. And this, by the way, is entirely apart from the factual concerns that have been raised about the adequacy of the security techniques that are deployed with this site for personal information.

THE COURT: All right. Let me get back, then, in terms of looking at the -- back to the standing issues in terms of -- you've indicated -- if you want to respond to what she indicated, why you would not be under the theory that it requires that there be this assessment before you collect -- no, it's the organizational. Excuse me. The organizational in terms of your public interest activities.

She indicated that -- and there was a distinction in terms of what are considered in that Public Interest Activities, what are allowed and what are not allowed in terms of providing you under this PETA case theory organizational standing.

If you want to respond to -- that's where your activities don't fit it.

MR. ROTENBERG: Right. Well, I think we've done this, Your Honor, in our reply brief, if I can just point to pages 20 and 21. In fact, we are relying on PETA in making the argument that we do have organizational standing and the activities we describe is the participation and work of our experts and to seek records from the Commission and to respond to the requests that had been made by the public.

What the language from PETA is relevant on this point is that our activities are, quote, "In response to and to counteract the effects of defendant's alleged unlawful conduct."

That's page 20 in the reply.

THE COURT: All right. The other question that I had is -- obviously, there needs to be some sort of federal agency connection to the Commission in order for the E-Gov Act to apply. So what is your best argument as to what federal agency is associated with it?

MR. ROTENBERG: Well, we think the Commission itself is an agency for purposes of the E-Government Act. That agency tracks the definition of the Freedom of Information Act and includes the Executive Office of the President.

So, therefore, the obligation to complete the Privacy Impact Assessment would fall upon the Commission as an agency.

THE COURT: You know, there is a case that talks about -- and I forgot which of the -- it was in the, I believe, the vice president's office, and it indicated that they provided basically personnel issues, those kinds of assistance. It was the executive office of either the president or the vice president. I forgot which, and it was -- that commission had not viewed itself as a federal agency.

MR. ROTENBERG: I'm not familiar with the case, Your Honor. If we could find the cite, we would be happy to provide a response.

I do want to point out, also --

THE COURT: Let me find it for you. It was *Crew vs. The Office Of Administration*. It was the Office of Administration within the Executive Office of the President. In fact, it was one of my cases relating to disclosure of documents to the White House's alleged loss of millions of emails, and they found that that commission, based on its functions, was not -- you know, was not considered a federal agency

for different purposes.

MR. ROTENBERG: All right. But I don't think that case implicated either the E-Government Act or the Federal Advisory Committee Act. So at least in the first instance, we would need to look at whether those statutes are relevant in Crew. I would be happy to look more closely, Your Honor.

THE COURT: Okay. So besides indicating that you think the Commission itself is a federal agency, any other argument?

MR. ROTENBERG: Well, yes. The GSA, in providing functional services to the Commission, which, as we set out we believe is the expectation contained within the executive order and also the charter of the Commission, would be subject to the agency status. And as you have also suggested, the member of the EAC, by virtue of the association with the EAC, could raise agency concerns.

We found it interesting, for example, that the Election Assistance Commission, not this commission, but the one that Ms. McCormick is a member of, has been subject to scrutiny under the Privacy Impact Assessment by that agency's

Office of Inspector General for similar activity.

Now, there's no wrongdoing. That's not what I'm suggesting. But, rather, the point being with far less data collection at the EAC, for more than 10 years the Office of Inspector General has paid careful attention to the E-Government obligation. That is my point.

THE COURT: But the problem, at least as she presents -- as Ms. Federighi presents it, is that the person that's on the Commission is not there in her official capacity.

MR. ROTENBERG: That's the representation.

THE COURT: Well, I know, but do you have something to counter it?

MR. ROTENBERG: Well, the person who is on the Commission is also affiliated with the most significant election commission apart from the president's commission that would address these issues.

THE COURT: Do you think -- the Department of Defense is not a defendant in this case, but is there any argument as we pursued this issue of the DOD having basically the website and all of this material uploaded to it and maintaining

it at least for a period of time until it gets transferred?

MR. ROTENBERG: Well --

THE COURT: Is that an agency that you would argue is involved with the Commission or not? Do you agree with the argument that it's not?

MR. ROTENBERG: We would say that, in fact, it is involved by virtue of the letter from the vice chair. But by law, under the executive order, it should not be involved. The fact that it is receiving data, and is most certainly subject to the Government Act as is evidenced by the fact they've already had a Privacy Impact Assessment, that is relevant. But the Privacy Impact Assessment reveals that the military website is not set up to receive the personal data that the vice chairman is seeking.

THE COURT: Well, I'm trying to see whether there is -- you agree with her argument that you view that it shouldn't be there. That doesn't get me anywhere in terms of your argument that the Commission is subject to the E-Gov Act. I still need a connection to a federal agency. So I'm just trying to figure

out whether that's an argument you're making or not making.

MR. ROTENBERG: Yes. Well, I would rely in part on opposing counsel's comment that the State of Arkansas has, in fact, transmitted voter data to the military website. So the fact that the military website is now in possession of that data beyond what the authorities provided in the Privacy Impact Assessment under which it is currently operating, and we would argue as well beyond the authority set out in the executive order in the Commission charter, necessarily makes it relevant to the proceeding.

THE COURT: All right. Anything else either one of you wants to say? I'm going to take a very short break. I know we're at 5:00, but I need to take a short break and figure out what additional questions, if any, I want to make because I would like to have this be the only hearing, and I'll go through all the information that you've got and then make a ruling.

MR. ROTENBERG: Thank you, Your Honor.

Just very briefly. We raised five counts. There is the Privacy Impact Assessment that

should've been completed. There's the Privacy Impact Assessment that was required as a condition of receiving the data. There is the obligation to publish that privacy impact under the Federal Advisory Committee Act, and we believe the informational privacy constitutional claims are actually quite strong here, and we would like the opportunity at some point to be able --

THE COURT: At this point, to make a constitutional argument I don't think you're going to do well in this circuit.

MR. ROTENBERG: I understand, Your Honor. Thank you.

THE COURT: Okay.

Anything you want to say at the end? I'm going to hear whatever you have to say, and then I need to take a quick break and look through and make sure -- I did a scramble of a bunch of notes because you've been filing things one after the other in terms of my being able to look through it to make sure that this is it and I have the information I need.

MS. SHAPIRO: Yes. Just very briefly. I just wanted to make two points. One is that

using the SAFE site as a tool I don't think makes that part of the Commission's work. It would be like saying that the Commission can use the post office to mail letters because that would make the post office somehow part of the Commission. It is a tool for getting the information.

THE COURT: Well, it's not getting the information. I mean, as a practical matter -- are you talking about the computer? The DOD thing?

MS. SHAPIRO: Yes.

THE COURT: Well, you're uploading it. They're maintaining the information. I don't know that I'd call it a tool as the post office would be.

I would agree, mailing things through the post office is not going to make them a federal agency as part of the Commission.

MS. SHAPIRO: And my second point is I wanted to just make clear the cases that set out the tests for the agency requirements, in other words, the functional test. The case that you referred to, the *Crew vs. Office Of Administration*, the case that Your Honor

handled, that involved the Office of Administration within the Executive Office of the President, was determined not to be an agency subject to FOIA. And the E-Government Act uses the same definition. That's the point I wanted to make clear, that the definition of agency is the same that's in FOIA. So the whole including the Executive Office of the President, we go back to the line of cases of *Soucie v. David*, *Mayer v. Bush*, which I think is the task force that Your Honor was referring to. That was the deregulation Reagan task force with the vice president as chair. So you have the *Mayer v. Bush*, the *Soucie vs. David*.

So all of those cases mean that the E-Government Act has to apply that same body of case law, and there's -- the functional test that's described in our papers, and we think is very clear that it's not satisfied here.

And the Armstrong case, in addition, makes it clear that just the mere participation of one person doesn't change the character.

THE COURT: Okay. Let me take a short break. I'll figure out if there's anything else, and I'll come back out.

MS. SHAPIRO: Thank you.

(Break.)

THE COURT: I have just one last question. I have not had an opportunity to review really carefully the last missive that I received from plaintiffs. I did look quickly through and noticed the DOD impact statement. So I need to go through and look at all of it more carefully. But if on reflection, in looking at it and reviewing the cases again and considering the arguments that were made and the answers that were given, if I decide that DOD is the federal agency connection to the Commission, since DOD is not a defendant, does it have to be a defendant in order for the Court to basically -- assuming I find standing -- to be able to issue any kind of order since they're the ones at this point maintaining the data on behalf of the Commission?

They're not a defendant now. Would they have to be if I made that decision? I'm not saying I'm going to. I'm just saying if I decided to do it.

Anybody have a position on that?

MR. ROTENBERG: Of course, we just learned

this afternoon that the DOD now possesses data. So we could quickly amend our complaint and add the DOD as a named defendant.

THE COURT: Okay. Any position from DOJ on this?

MS. SHAPIRO: Our position would be that the Court would not be empowered to enter relief against a nonparty so that --

THE COURT: Right. Okay. He would have to make a decision as to whether he wanted to amend the complaint. Let's assume he filed a motion to amend the complaint which would include DOD, what would your position be?

MS. SHAPIRO: That it --

THE COURT: I mean, presumably, at this point they possess data, right? And they're maintaining it, at least at this point?

MS. SHAPIRO: For some ephemeral amount of time.

THE COURT: But they still have it at this point. So if they decided to amend it, I mean, then the Court would have to see whether that works anyway. But I'm just saying that it's clear that if they're not a party, I would not be able to act if I thought that was the -- or

concluded that that was the federal agency connection.

So if they filed a motion to do it, what would your answer be?

MS. SHAPIRO: Well, I think we would respond with arguments similar that the DOD tool that is being used does not convert -- make any difference to the agency -- to the Commission's status as a non-agency or a requirement to do a Privacy Impact Assessment.

THE COURT: So that would -- all right. In terms of doing it, but it doesn't get to whether -- even if he decided to put it in, it doesn't mean that he necessarily will decide that.

So it seems to me, since at this point they do have the data, and they're maintaining it, that they could certainly have grounds to put them in as a party. It doesn't mean I necessarily am going to find, as they would hope, that that is the federal agency connection. But I just wanted to make sure if I started to go down that path, it actually could -- it could be any ruling.

MS. SHAPIRO: I'm sorry. I didn't

understand the last --

THE COURT: All right. I brought this up because this has been a more developed argument about DOD and its role, since that's come out really only in recent times, and the exhibit I got at 3:00. So I haven't had too long to look at it in terms of what's involved with it. And you have indicated that it, at this point, holds data from the State of Arkansas. So it has the information, and it's maintaining it on behalf of the Commission. So that presumably would be their reason to amend it. The Court would still have to make these other decisions. It doesn't change it.

MS. SHAPIRO: Correct.

THE COURT: I just want to see that if I decided to do that, that I actually would be in a position to do it.

MS. SHAPIRO: Okay.

THE COURT: All right. So if you're going to amend it, you need to move swiftly. All right. I don't have anything else, and so I will excuse you.

I will not be doing an oral ruling. Obviously, it's very complicated. I will be

doing something in writing. I will get it out as quickly as I can understanding the time lines that have been set out.

All right? Thank you. Take care.

(Hearing concluded.)

CERTIFICATE OF REPORTER

I, Richard D. Ehrlich, a Registered Merit Reporter and Certified Realtime Reporter, certify that the foregoing is a true, complete, and accurate transcript of the proceedings ordered to be transcribed in the above-entitled case before the Honorable Colleen Kollar-Kotelly, in Washington, DC, on July 7, 2017.

s/Richard D. Ehrlich July 10, 2017

Richard D. Ehrlich, Official Court Reporter

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*, Defendants.	Civil Action No. 1:17-cv-1320 (CKK)

THIRD DECLARATION OF KRIS W. KOBACH

I, Kris W. Kobach, declare as follows:

As described in my declaration of July 5, 2017, I am the Vice Chair of the Presidential Advisory Commission on Election Integrity ("Commission"). I submit this third declaration in support of Defendant's supplemental brief regarding the addition of the Department of Defense ("DOD") as a defendant in plaintiff's Amended Complaint. This declaration is based on my personal knowledge and upon information provided to me in my official capacity as Vice Chair of the Commission.

1. In order not to impact the ability of other customers to use the DOD Safe Access File Exchange ("SAFE") site, the Commission has decided to use alternative means for transmitting the requested data. The Commission no longer intends to use the DOD SAFE system to receive information from the states, and instead intends to use alternative means of receiving the information requested in the June 28, 2017, letter. Specifically, the Director of White House Information Technology is repurposing an existing system that regularly accepts

personally identifiable information through a secure, encrypted computer application within the White House Information Technology enterprise. We anticipate this system will be fully functional by 6:00 p.m. Eastern today.

2. Today, the Commission sent the states a follow-up communication requesting the states not submit any data until this Court rules on this TRO motion. A copy of this communication is attached hereto as Exhibit A. The Commission will not send further instructions about how to use the new system pending this Court's resolution of this TRO motion.

3. The Commission will not download the data that Arkansas already transmitted to SAFE and this data will be deleted from the site.

4. Additionally, I anticipate that the President will today announce the appointment of two new members of the Commission, one Democrat and one Republican.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

***

Executed this 10th day of July 2017.

Kris Kobach

Kris W. Kobach

From: FN-OVP-Election Integrity Staff
Sent: Monday, July 10, 2017 9:40 AM
Subject: Request to Hold on Submitting Any Data Until Judge Rules on TRO

Dear Election Official,

As you may know, the Electronic Privacy Information Center filed a complaint seeking a Temporary Restraining Order ("TRO") in connection with the June 28, 2017 letter sent by Vice Chair Kris Kobach requesting publicly-available voter data. See *Electronic Privacy Information Center v. Presidential Advisory Commission on Election Integrity* filed in the U.S. District Court for the District of Columbia. Until the Judge rules on the TRO, we request that you hold on submitting any data. We will follow up with you with further instructions once the Judge issues her ruling.

Andrew Kossack
Designated Federal Officer
Presidential Advisory Commission on Election Integrity
ElectionIntegrityStaff@ovp.eop.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009

Plaintiff,

v.

Civ. Action No. 17-1320 (CKK)

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY; MICHAEL PENCE, in his official capacity as Chair of the Presidential Advisory Commission on Election Integrity; KRIS KOBACH, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; CHARLES C. HERNDON, in his official capacity as Director of White House Information Technology; EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES; OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES; UNITED STATES DIGITAL SERVICE; EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY;
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

GENERAL SERVICES ADMINISTRATION
1800 F Street, N.W.
Washington, D.C. 20405

UNITED STATES DEPARTMENT OF DEFENSE
1000 Defense Pentagon
Washington, D.C. 20301-0001

Defendants.

SECOND AMENDED COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Administrative Procedure Act ("APA"), 5 U.S.C. §§ 551–706, the Federal Advisory Committee Act ("FACA"), 5 U.S.C. app. 2, and the United States Constitution for injunctive and other appropriate relief to halt the collection of state voter data by the Presidential Advisory Commission on Election Integrity (the "PACEI" or the "Commission"), by officers of the Commission, and by the agencies which oversee and facilitate the activities of the Commission, including the Department of Defense.

2. The Electronic Privacy Information Center ("EPIC") challenges the Defendants' intent to collect the personal data of millions of registered voters and to publish partial SSNs as an unconstitutional invasion of privacy and a violation of the obligation to conduct a Privacy Impact Assessment ("PIA").

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, 5 U.S.C. § 702, and 5 U.S.C. § 704. This Court has personal jurisdiction over Defendants.

4. Venue is proper in this district under 5 U.S.C. § 703 and 28 U.S.C. § 1391.

Parties

5. Plaintiff EPIC is a nonprofit organization incorporated in Washington, D.C., and established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities. EPIC's Advisory Board members include distinguished experts in law, technology, public policy, and cybersecurity. EPIC has a long history of working to protect voter privacy and the security of election infrastructure. EPIC has specific expertise regarding the misuse of the Social Security Number ("SSN") and has sought stronger protections for the SSN for more than two decades.

6. EPIC's members include registered voters in California, the District of Columbia, Florida, Maryland, Massachusetts, Minnesota, New York, Pennsylvania, Texas, and Washington.

7. Defendant PACEI is an advisory committee of the U.S. government within the meaning of FACA, 5 U.S.C. app. 2 § 10. Defendant PACEI is also an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

8. Defendant Michael Pence is the Vice President of the United States and the Chair of the PACEI.

9. Defendant Kris Kobach is the Secretary of State of Kansas and the Vice Chair of the PACEI.

10. Defendant Charles C. Herndon is the Director of White House Information Technology.

11. Defendant Executive Office of the President of the United States ("EOP") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

12. Defendant U.S. Digital Service is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

13. Defendant Executive Committee for Presidential Information Technology consists of the following officials or their designees: the Assistant to the President for Management and Administration; the Executive Secretary of the National Security Council; the Director of the Office of Administration; the Director of the United States Secret Services; and the Director of the White House Military Office. The Executive Committee is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

14. Defendant Office of the Vice President of the United States ("OVP") is a subcomponent of EOP and an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

15. Defendant General Services Administration ("GSA") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701. The GSA is charged with providing the PACEI

"such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission . . . ." Ex. 1.[1]

16. Defendant United States Department of Defense ("DoD") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701. The DoD manages and controls the Safe Access File System ("SAFE").

Facts

The Commission's Unprecedented Collection of State Voter Data

17. The Commission was established by Executive Order on May 11, 2017 ("Commission Order"). Ex 1.[2]

18. The Commission is charged with "study[ing] the registration and voting processes used in Federal elections." Ex. 1.[3] The Commission Order contains no authority to gather personal data or to undertake investigations.[4]

19. On June 28, 2017, the Vice Chair of the Commission undertook to collect detailed voter histories from all fifty states and the District of Columbia. Such a request had never been made by any federal official in the history of the country. The Vice Chair stated during a phone call with Commission members that "a letter w[ould] be sent today to the 50 states and District of Columbia on behalf of the Commission requesting publicly-available data from state voter rolls . . ." Ex. 2.[5]

---

[1] Exec. Order. No. 13,799, 82 Fed. Reg. 22,389, 22,390 (May 11, 2017).
[2] 82 Fed. Reg. at 22,389; *see also Voter Privacy and the PACEI*, EPIC.org (June 30, 2017), https://epic.org/privacy/voting/pacei/.
[3] 82 Fed. Reg. at 22,389.
[4] *See generally id.*
[5] Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017).

20. According to the U.S. Census, state voter rolls include the names, addresses, and other personally identifiable information of at least 157 million registered voters.[6]

21. One of the letters from the Commission, dated June 28, 2017, was sent to North Carolina Secretary of State Elaine Marshall. Ex. 3.[7]

22. In the letter ("Commission Letter"), the Vice Chair urged the Secretary of State to provide to the Commission the "full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information." Ex. 3.[8]

23. The Commission Letter also asked "[w]hat evidence or information [the state had] regarding instances of voter fraud or registration fraud" and "[w]hat convictions for election-related crimes ha[d] occurred in [the] state since the November 2000 federal election." Ex. 3.[9]

24. The Commission Letter stated that "any documents that are submitted to the full Commission w[ould] also be made available to the public." Ex. 3.[10]

25. The Commission asked for a response by July 14, 2017. Ex. 3.[11] The "SAFE" URL, recommend by the Commission for the submission of voter data, leads election officials to a non-

---

[6] U.S. Census Bureau, *Voting and Registration in the Election of November 2016* at tbl. 4a (May 2017), https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-580.html.
[7] Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017).
[8] *Id.* at 1–2.
[9] *Id.* at 1.
[10] *Id.* at 2.
[11] *Id.*

secure site. Regarding this website, Google Chrome states: "Your connection is not private. Attackers may be trying to steal your information from [the site proposed by the Commission] (for example, passwords, messages, or credit cards)." Ex. 4.[12]

26. As of July 7, 2017, the Department of Defense has received voter data from at least one state, Arkansas, in the SAFE system.

27. According to representations made by the Commission in the July 10, 2017 response, the Commission sent a "Follow-up Communication" to the states, requesting that the States not submit any data until this Court rules on EPIC's motion for a temporary restraining order.

28. The Follow-up Communication from the Commission to the States was not made public as would be required by the Federal Advisory Committee Act.

29. There is no public confirmation that all of the States received the Follow-up Communication from the Commission.

30. There is no public confirmation that the States that did receive the Follow-up Communication will comply.

31. According to representations made by the Commission in the July 10, 2017 response, the Director of White House Information Technology is "repurposing" a computer system to be used for collecting personal voter data.

32. On July 10, 2017, the Commission stated that it would not send further instructions about how to use the new system pending the Court's resolution of EPIC's motion for a temporary restraining order.

[12] Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Site (July 3, 2017 12:02 AM).

33. On July 10, 2017, the Commission stated that it would not download the data that Arkansas already transmitted via the DoD system, and that the data will be deleted from the site. There has been no confirmation that the data has been deleted.

The General Service Administration's Role in Providing Support to the Commission

34. The Executive Order provides that the GSA "shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis."[13]

35. The Commission Charter designates the GSA as the "Agency Responsible for Providing Support," and similarly orders that the GSA "shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis."[14]

36. The GSA routinely conducts and publishes Privacy Impact Assessments when it collects, maintains, and uses personal information on individuals.[15]

37. There is no authority in the Executive Order of the Commission Charter for any other entity to provide "administrative services," "facilities," or "equipment" to "carry out [the Commission's] mission."

Many States Oppose the Commission's Demand for Personal Voter Data

38. In less than three days following the release of the Commission Letter, election officials in twenty-four states said that they would oppose, partially or fully, the demand for personal voter data.[16]

---

[13] 82 Fed. Reg. at 22,390.
[14] Charter, Presidential Advisory Commission on Election Integrity ¶ 6.
[15] *Privacy Impact Assessments*, GSA (Apr. 13, 2017), https://www.gsa.gov/portal/content/102237.

39. California Secretary of State Alex Padilla stated that he would "not provide sensitive voter information to a committee that has already inaccurately passed judgment that millions of Californians voted illegally. California's participation would only serve to legitimize the false and already debunked claims of massive voter fraud."[17]

40. Kentucky Secretary of State Alison Lundergan Grimes stated that "Kentucky w[ould] not aid a commission that is at best a waste of taxpayer money and at worst an attempt to legitimize voter suppression efforts across the country."[18]

41. Virginia Governor Terry McAuliffe stated that he had "no intention of honoring [Kobach's] request."[19]

42. More than fifty experts in voting technology and twenty privacy organizations wrote to state election officials to warn that "[t]here is no indication how the information will be used, who will have access to it, or what safeguards will be established."[20]

Failure to Conduct a Privacy Impact Assessment

---

[16] Philip Bump & Christopher Ingraham, *Trump Says States Are 'Trying to Hide' Things from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/.

[17] Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017), http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/.

[18] Bradford Queen, Secretary Grimes Statement on Presidential Election Commission's Request for Voters' Personal Information, Kentucky (last accessed July 3, 2017) http://kentucky.gov/Pages/Activity-stream.aspx?n=SOS&prId=129.

[19] Terry McAuliffe, *Governor McAuliffe Statement on Request from Trump Elections Commission* (June 29, 2017), https://governor.virginia.gov/newsroom/newsarticle?articleId=20595.

[20] Letter from EPIC et al. to Nat'l Ass'n of State Sec'ys (July 3, 2017), https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf.

43. Under the E-Government Act of 2002,[21] any agency "initiating a new collection of information that (I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual" is required to complete a Privacy Impact Assessment ("PIA") before initiating such collection.[22]

44. The agency must "(i) conduct a privacy impact assessment; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."[23]

45. The Commission is an agency subject to the E-Government Act because it is an "establishment in the executive branch of the Government," a category which "includ[es] the Executive Office of the President."[24]

46. The Executive Office of the President is an agency subject to the E-Government Act.

47. The U.S. Digital Service is an agency subject to the E-Government Act.

48. The Director of White House Information Technology is subject to the E-Government Act.

49. The Director of White House Information Technology was established in 2015 and has "the primary authority to establish and coordinate the necessary policies and procedures for

[21] Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note).
[22] 44 U.S.C. § 3501 note ("Privacy Impact Assessments").
[23] *Id.*
[24] 44 U.S.C. § 3502(1).

operating and maintaining the information resources and information systems provided to the President, Vice President, and EOP."[25] This authority includes:

> providing "policy coordination and guidance for, and periodically review[ing], all activities relating to the information resources and information systems provided to the President, Vice President, and EOP by the Community, including expenditures for, and procurement of, information resources and information systems by the Community. Such activities shall be subject to the Director's coordination, guidance, and review in order to ensure consistency with the Director's strategy and to strengthen the quality of the Community's decisions through integrated analysis, planning, budgeting, and evaluating process.[26]

The Director may also "advise and confer with appropriate executive departments and agencies, individuals, and other entities as necessary to perform the Director's duties under this memorandum."[27]

50. The Director has the independent authority to oversee and "provide the necessary advice, coordination, and guidance to" the Executive Committee for Presidential Information Technology, which "consists of the following officials or their designees: the Assistant to the President for Management and Administration; the Executive Secretary of the National Security Council; the Director of the Office of Administration; the Director of the United States Secret Service; and the Director of the White House Military Office."[28]

51. A Privacy Impact Assessment for a "new collection of information" must be "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information."[29] The PIA must specifically address "(I) what information is to be

---

[25] Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology § 1, 2015 Daily Comp. Pres. Doc. 185 (Mar. 19, 2015), attached as Ex. 5.
[26] *Id.* § 2(c).
[27] *Id.* § 2(d).
[28] *Id.* § 3.
[29] 44 U.S.C. § 3501 note ("Privacy Impact Assessments").

collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and] (VI) how the information will be secured . . . ."[30]

52. Under the FACA, "records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by [an] advisory committee shall be available for public inspection and copying at a single location in the offices of the advisory committee or the agency to which the advisory committee reports until the advisory committee ceases to exist."[31]

53. None of the Defendants have conducted a Privacy Impact Assessment for the Commission's collection of state voter data.

54. None of the Defendants have ensured review of a PIA by any Chief Information Officer or equivalent official.

55. The Commission has not published a PIA or made such an assessment available for public inspection.

The DoD's Privacy Impact Assessment Does Not Permit
the Collection of Personal Information from The General Public

56. The DoD last approved a PIA for the Safe Access File Exchange system in 2015.[32]

57. The 2015 PIA indicates that the SAFE system may "collect, maintain, use and/or disseminate PII" about only "federal personnel and/or federal contractors."[33]

---

[30] *Id.*
[31] 5 U.S.C. app. 2 § 10(b).
[32] Army Chief Information Officer, U.S. Dep't of Def., *Privacy Impact Assessments* (April 27, 2016), http://ciog6.army.mil/PrivacyImpactAssessments/tabid/71/Default.aspx.
[33] EPIC Supp. Ex. 5, ECF No. 20-1, at 1.

58. The 2015 PIA specifically indicates that the SAFE system may not be used to "collect, maintain, use and/or disseminate PII" from "members of the general public."[34]

59. According to the 2015 PIA, the SAFE system may not be used to collect the data set out in the June 28, 2017, from Vice Chair Kobach, directing state election officials to provide voter roll data.

60. The DoD has not issued a PIA for the collection of personal data from the general public.

61. The DoD has not issued a PIA that would permit the receipt of data specified in the June 28, 2017, Kobach letter.

Count I

Violation of APA: Unlawful Agency Action

62. Plaintiff asserts and incorporates by reference paragraphs 1–42.

63. Defendants' collection of state voter data prior to creating, reviewing, and publishing a Privacy Impact Assessment, 44 U.S.C. § 3501 note, is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law under 5 U.S.C. § 706(2)(a) and short of statutory right under 5 U.S.C. § 706(2)(c).

64. Defendants' decision to initiate collection of voter data is a final agency action within the meaning of 5 U.S.C. § 704.

65. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions.

66. Plaintiff has exhausted all applicable administrative remedies.

Count II

Violation of APA: Agency Action Unlawfully Withheld

[34] EPIC Supp. Ex. 5, ECF No. 20-1, at 1.

67. Plaintiff asserts and incorporates by reference paragraphs 1–42.

68. Defendants have failed to create, review, and/or publish a privacy impact assessment for Defendants' collection of voter data, as required by 44 U.S.C. § 3501 note and 5 U.S.C. app. 2 § 10(b).

69. Defendants' failure to take these steps constitutes agency action unlawfully withheld or unreasonably delayed in violation of 5 U.S.C. § 706(1).

70. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

71. Plaintiff has exhausted all applicable administrative remedies.

Count III

Violation of FACA: Failure to Make Documents Available for Public Inspection

72. Plaintiff asserts and incorporates by reference paragraphs 1–42.

73. Defendants have failed to make available for public inspection a privacy impact assessment for the collection of voter data.

74. Defendants' failure to make available for public inspection a PIA required by law is a violation of 5 U.S.C. app. 2 § 10(b).

75. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

76. Plaintiff has exhausted all applicable administrative remedies.

Count IV

Violation of Fifth Amendment: Substantive Due Process/Right to Informational Privacy

77. Plaintiff asserts and incorporates by reference paragraphs 1–42.

78. Defendants, by seeking to assemble an unnecessary and excessive federal database of sensitive voter data from state records systems, have violated the informational privacy rights of millions of Americans, including members of the EPIC Advisory Board, guaranteed by the Due Process Clause of the Fifth Amendment. *See* U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

79. Plaintiff, as a representative of its members, is adversely affected and aggrieved by Defendants' actions.

Count V

Violation of Fifth Amendment: Procedural Due Process

80. Plaintiff asserts and incorporates by reference paragraphs 1–42.

81. Defendants, by seeking to assemble an unnecessary and excessive federal database of sensitive voter data from state records systems, have deprived EPIC's members of their liberty interest in avoiding the disclosure of personal matters. U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

82. Defendants have done so without providing notice to EPIC's members, without providing EPIC's members an opportunity to challenge the collection of their personal data, and without providing for a neutral decisionmaker to decide on any such challenges brought by EPIC's members.

83. Defendants have violated EPIC's members Fifth Amendment right to due process of law. U.S. Const. amend. V.

84. Plaintiff, as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

Requested Relief

WHEREFORE, Plaintiff requests that this Court:

A. Hold unlawful and set aside Defendants' authority to collect personal voter data from the states;

B. Order Defendants to halt collection of personal voter data;

C. Order Defendants to securely delete and properly disgorge any personal voter data collected or subsequently received;

D. Order Defendants to promptly conduct a privacy impact assessment prior to the collection of personal voter data;

E. Award EPIC costs and reasonable attorney's fees incurred in this action; and

F. Grant such other relief as the Court may deem just and proper.

Respectfully Submitted,

/s/ Marc Rotenberg
MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel

CAITRIONA FITZGERALD*
EPIC Policy Director

JERAMIE D. SCOTT, D.C. Bar # 1025909
EPIC Domestic Surveillance Project Director

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.

Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Plaintiff EPIC

** Pro hac vice motion pending*

Dated: July 11, 2017

This is historical material, "frozen in time" and not current OMB guidance.
The web site is no longer updated and links to external web sites and some internal pages will not work.

OFFICE OF MANAGEMENT AND BUDGET

September 26, 2003

M-03-22

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
DirectoR

SUBJECT: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

The attached guidance provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

The Administration is committed to protecting the privacy of the American people. This guidance document addresses privacy protections when Americans interact with their government. The guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

The privacy objective of the E-Government Act complements the National Strategy to Secure Cyberspace. As the National Strategy indicates, cyberspace security programs that strengthen protections for privacy and other civil liberties, together with strong privacy policies and practices in the federal agencies, will ensure that information is handled in a manner that maximizes both privacy and security.

Background

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act (see Attachment A). The text of section 208 is provided as Attachment B to this Memorandum. Attachment C provides a general outline of regulatory requirements pursuant to the Children's Online Privacy Protection Act ("COPPA"). Attachment D summarizes the modifications to existing guidance resulting from this Memorandum. A complete list of OMB privacy guidance currently in effect is available at OMB's website.

As OMB has previously communicated to agencies, for purposes of their FY2005 IT budget requests, agencies should submit all required Privacy Impact Assessments no later than October 3, 2003.

For any questions about this guidance, contact Eva Kleederman, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3647, fax (202) 395-5167, e-mail Eva_Kleederman@omb.eop.gov.

Attachments

Attachment A
Attachment B
Attachment C
Attachment D

Attachment A

E-Government Act Section 208 Implementation Guidance

I. General

A. ***Requirements.*** Agencies are required to:

1. conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available (see Section II of this Guidance),
2. post privacy policies on agency websites used by the public (see Section III),
3. translate privacy policies into a standardized machine-readable format (see Section IV), and
4. report annually to OMB on compliance with section 208 of the E-Government Act of 2002 (see Section VII).

B. ***Application.*** This guidance applies to:

1. all executive branch departments and agencies ("agencies") and their contractors that use information technology or that operate websites for purposes of interacting with the public;
2. relevant cross-agency initiatives, including those that further electronic government.

C.

Modifications to Current Guidance. Where indicated, this Memorandum modifies the following three memoranda, which are replaced by this guidance (see summary of modifications at Attachment D):

1. Memorandum 99-05 (January 7, 1999), directing agencies to examine their procedures for ensuring the privacy of personal information in federal records and to designate a senior official to assume primary responsibility for privacy policy;
2. Memorandum 99-18 (June 2, 1999), concerning posting privacy policies on major entry points to government web sites as well as on any web page collecting substantial personal information from the public; and
3. Memorandum 00-13 (June 22, 2000), concerning (i) the use of tracking technologies such as persistent cookies and (ii) parental consent consistent with the Children's Online Privacy Protection Act ("COPPA").

II. Privacy Impact Assessment

A. ***Definitions.***

1. *Individual* - means a citizen of the United States or an alien lawfully admitted for permanent residence.[1]
2. *Information in identifiable form*- is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).[2]
3. *Information technology (IT)* - means, as defined in the Clinger-Cohen Act[3], any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
4. *Major information system* - embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources.
5. *National Security Systems* - means, as defined in the Clinger-Cohen Act[4], an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.
6. *Privacy Impact Assessment (PIA)*- is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
7. *Privacy policy in standardized machine-readable format*- means a statement about site privacy

practices written in a standard computer language (not English text) that can be read automatically by a web browser.

B. ***When to conduct a PIA:***[5]

1. *The E-Government Act requires agencies to conduct a PIA before:*
   a. developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
   b. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).
2. *In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:*
   a. Conversions - when converting paper-based records to electronic systems;
   b. Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
   c. Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
      - For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
   d. Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
      - For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.
   e. New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
   f. Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
   g. New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
      - For example the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross agency IT investment.
   h. Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
      - For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.
   i. Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)
3. *No PIA is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged, as in the following circumstances:*
   a. for government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public (this includes government personnel and government contractors and consultants);[6]
   b. for government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or

obtaining additional information;
c. for national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act);
d. when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act (see 5 U.S.C. §§ 552a(8-10), (e)(12), (o), (p), (q), (r), (u)), which specifically provide privacy protection for matched information;
e. when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the E-Government Act of 2002;
f. if agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generates information in identifiable form;
g. for minor changes to a system or collection that do not create new privacy risks.

4. *Update of PIAs:* Agencies must update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

C. ***Conducting a PIA.***

1. *Content.*
   a. PIAs must analyze and describe:
      i. what information is to be collected (e.g., nature and source);
      ii. why the information is being collected (e.g., to determine eligibility);
      iii. intended use of the information (e.g., to verify existing data);
      iv. with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
      v. what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
      vi. how the information will be secured (e.g., administrative and technological controls[7]); and
      vii. whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.
   b. Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.
2. Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection:
   a. *Specificity.* The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.
      i. *IT development stage.* PIAs conducted at this stage:
         1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
         2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;
         3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.
      ii. *Major information systems.* PIAs conducted for these systems should reflect more extensive analyses of:
         1. the consequences of collection and flow of information,
         2. the alternatives to collection and handling as designed,
         3. the appropriate measures to mitigate risks identified for each alternative and,
         4. the rationale for the final design choice or business process.
      iii. *Routine database systems.* Agencies may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.
   b. *Information life cycle analysis/collaboration.* Agencies must consider the information "life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals' privacy. To be

comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy.

3. *Review and publication.*
   a. a. Agencies must ensure that:
      i. the PIA document and, if prepared, summary are approved by a "reviewing official" (the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA);
      ii. for each covered IT system for which 2005 funding is requested, and consistent with previous guidance from OMB, the PIA is submitted to the Director of OMB no later than October 3, 2003 (submitted electronically to PIA@omb.eop.gov along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 300[8]); and
      iii. the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).
         1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment[9]. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).
         2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

D. *Relationship to requirements under the Paperwork Reduction Act (PRA)*[10].
   1. Joint Information Collection Request (ICR) and PIA. Agencies undertaking new electronic information collections may conduct and submit the PIA to OMB, and make it publicly available, as part of the SF83 Supporting Statement (the request to OMB to approve a new agency information collection).
   2. If Agencies submit a Joint ICR and PIA:
      a. All elements of the PIA must be addressed and identifiable within the structure of the Supporting Statement to the ICR, including:
         i. a description of the information to be collected in the response to Item 1 of the Supporting Statement[11];
         ii. a description of how the information will be shared and for what purpose in Item 2 of the Supporting Statement[12];
         iii. a statement detailing the impact the proposed collection will have on privacy in Item 2 of the Supporting Statement[13];
         iv. a discussion in item 10 of the Supporting Statement of:
            1. whether individuals are informed that providing the information is mandatory or voluntary
            2. opportunities to consent, if any, to sharing and submission of information;
            3. how the information will be secured; and
            4. whether a system of records is being created under the Privacy Act)[14].
      b. For additional information on the requirements of an ICR, please consult your agency's organization responsible for PRA compliance.
   3. Agencies need not conduct a new PIA for simple renewal requests for information collections under the PRA. As determined by reference to section II.B.2. above, agencies must separately consider the need for a PIA when amending an ICR to collect information that is significantly different in character from the original collection.

E. *Relationship to requirements under the Privacy Act of 1974, 5 U.S. C. 552a.*

   1. Agencies may choose to conduct a PIA when developing the System of Records (SOR) notice required by subsection (e)(4) of the Privacy Act, in that the PIA and SOR overlap in content (e.g., the categories of records in the system, the uses of the records, the policies and practices for handling, etc.).
   2. Agencies, in addition, may make the PIA publicly available in the Federal Register along with the Privacy Act SOR notice.

3. Agencies must separately consider the need for a PIA when issuing a change to a SOR notice (e.g., a change in the type or category of record added to the system may warrant a PIA).

III. Privacy Policies on Agency Websites

A. *Privacy Policy Clarification.* To promote clarity to the public, agencies are required to refer to their general web site notices explaining agency information handling practices as the "Privacy Policy."

B. *Effective Date.* Agencies are expected to implement the following changes to their websites by December 15, 2003.

C. *Exclusions:* For purposes of web privacy policies, this guidance does not apply to:
1. information other than "government information" as defined in OMB Circular A-130;
2. agency intranet web sites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees);
3. national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-government Act).

D. *Content of Privacy Policies.*
1. Agency Privacy Policies must comply with guidance issued in OMB Memorandum 99-18 and must now also include the following two new content areas:
   a. *Consent to collection and sharing*[15]. Agencies must now ensure that privacy policies:
      i. inform visitors whenever providing requested information is voluntary;
      ii. inform visitors how to grant consent for use of voluntarily-provided information; and
      iii. inform visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.
   b. *Rights under the Privacy Act or other privacy laws*[16]. Agencies must now also notify web-site visitors of their rights under the Privacy Act or other privacy-protecting laws that may primarily apply to specific agencies (such as the Health Insurance Portability and Accountability Act of 1996, the IRS Restructuring and Reform Act of 1998, or the Family Education Rights and Privacy Act):
      i. in the body of the web privacy policy;
      ii. via link to the applicable agency regulation (e.g., Privacy Act regulation and pertinent system notice); or
      iii. via link to other official summary of statutory rights (such as the summary of Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at www.Firstgov.gov).
2. Agency Privacy Policies must continue to address the following, modified, requirements:
   a. Nature, purpose, use and sharing of information collected . Agencies should follow existing policies (issued in OMB Memorandum 99-18) concerning notice of the nature, purpose, use and sharing of information collected via the Internet, as modified below:
      i. *Privacy Act information.* When agencies collect information subject to the Privacy Act, agencies are directed to explain what portion of the information is maintained and retrieved by name or personal identifier in a Privacy Act system of records and provide a Privacy Act Statement either:
         1. at the point of collection, or
         2. via link to the agency's general Privacy Policy[18].
      ii. *"Privacy Act Statements."* Privacy Act Statements must notify users of the authority for and purpose and use of the collection of information subject to the Privacy Act, whether providing the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.
      iii. *Automatically Collected Information (site management data).* Agency Privacy Policies must specify what information the agency collects automatically (i.e., user's IP address, location, and time of visit) and identify the use for which it is collected (i.e., site management or security purposes).
      iv. *Interaction with children:* Agencies that provide content to children under 13 and that collect personally identifiable information from these visitors should incorporate the requirements of the Children's Online Privacy Protection Act ("COPPA") into their Privacy Policies (see Attachment C)[19].
      v. *Tracking and customization activities.* Agencies are directed to adhere to the following modifications to OMB Memorandum 00-13 and the OMB follow-up guidance letter dated September 5, 2000:
         1. *Tracking technology prohibitions:*

a. agencies are prohibited from using persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Internet except as provided in subsection (b) below;
b. agency heads may approve, or may authorize the heads of sub-agencies or senior official(s) reporting directly to the agency head to approve, the use of persistent tracking technology for a compelling need. When used, agency's must post clear notice in the agency's privacy policy of:
    - the nature of the information collected;
    - the purpose and use for the information;
    - whether and to whom the information will be disclosed; and
    - the privacy safeguards applied to the information collected.
c. agencies must report the use of persistent tracking technologies as authorized for use by subsection b. above (see section VII)[20].

2. *The following technologies are not prohibited:*
    a. Technology that is used to facilitate a visitor's activity within a single session (e.g., a "session cookie") and does not persist over time is not subject to the prohibition on the use of tracking technology.
    b. Customization technology (to customize a website at the visitor's request) if approved by the agency head or designee for use (see v.1.b above) and where the following is posted in the Agency's Privacy Policy:
        - the purpose of the tracking (i.e., customization of the site);
        - that accepting the customizing feature is voluntary;
        - that declining the feature still permits the individual to use the site; and
        - the privacy safeguards in place for handling the information collected.
    c. Agency use of password access to information that does not involve "persistent cookies" or similar technology.

vi. *Law enforcement and homeland security sharing:* Consistent with current practice, Internet privacy policies may reflect that collected information may be shared and protected as necessary for authorized law enforcement, homeland security and national security activities.

b. *Security of the information*[21]. Agencies should continue to comply with existing requirements for computer security in administering their websites[22] and post the following information in their Privacy Policy:
    i. in clear language, information about management, operational and technical controls ensuring the security and confidentiality of personally identifiable records (e.g., access controls, data storage procedures, periodic testing of safeguards, etc.), and
    ii. in general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems. (The statement should be at a level to inform the public that their information is being protected while not compromising security.)

E. *Placement of notices.* Agencies should continue to follow the policy identified in OMB Memorandum 99-18 regarding the posting of privacy policies on their websites. Specifically, agencies must post (or link to) privacy policies at:
    1. their principal web site;
    2. any known, major entry points to their sites;
    3. any web page that collects substantial information in identifiable form.
F. ***Clarity of notices.*** Consistent with OMB Memorandum 99-18, privacy policies must be:
    1. clearly labeled and easily accessed;
    2. written in plain language; and
    3. made clear and easy to understand, whether by integrating all information and statements into a single posting, by layering a short "highlights" notice linked to full explanation, or by other means the agency determines is effective.

IV. Privacy Policies in Machine-Readable Formats

A. ***Actions.***
    1. Agencies must adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make

an informed choice about whether to conduct business with that site.
2. OMB encourages agencies to adopt other privacy protective tools that become available as the technology advances.

B. ***Reporting Requirement.*** Agencies must develop a timetable for translating their privacy policies into a standardized machine-readable format. The timetable must include achievable milestones that show the agency's progress toward implementation over the next year. Agencies must include this timetable in their reports to OMB (see Section VII).

V. Privacy Policies Incorporated by this Guidance

In addition to the particular actions discussed above, this guidance reiterates general directives from previous OMB Memoranda regarding the privacy of personal information in federal records and collected on federal web sites. Specifically, existing policies continue to require that agencies:

A. assure that their uses of new information technologies sustain, and do not erode, the protections provided in all statutes relating to agency use, collection, and disclosure of personal information;
B. assure that personal information contained in Privacy Act systems of records be handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
C. evaluate legislative proposals involving collection, use and disclosure of personal information by the federal government for consistency with the Privacy Act of 1974;
D. evaluate legislative proposals involving the collection, use and disclosure of personal information by any entity, public or private, for consistency with the Privacy Principles;
E. ensure full adherence with stated privacy policies.

VI. Agency Privacy Activities/Designation of Responsible Official

Because of the capability of information technology to capture and disseminate information in an instant, all federal employees and contractors must remain mindful of privacy and their obligation to protect information in identifiable form. In addition, implementing the privacy provisions of the E-Government Act requires the cooperation and coordination of privacy, security, FOIA/Privacy Act and project officers located in disparate organizations within agencies. Clear leadership and authority are essential.

Accordingly, this guidance builds on policy introduced in Memorandum 99-05 in the following ways:

A. Agencies must:
   1. inform and educate employees and contractors of their responsibility for protecting information in identifiable form;
   2. identify those individuals in the agency (e.g., information technology personnel, Privacy Act Officers) that have day-to-day responsibility for implementing section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies.
   3. designate an appropriate senior official or officials (e.g., CIO, Assistant Secretary) to serve as the agency's principal contact(s) for information technology/web matters and for privacy policies. The designated official(s) shall coordinate implementation of OMB web and privacy policy and guidance.
   4. designate an appropriate official (or officials, as appropriate) to serve as the "reviewing official(s)" for agency PIAs.

B. OMB leads a committee of key officials involved in privacy that reviewed and helped shape this guidance and that will review and help shape any follow-on privacy and web-privacy-related guidance. In addition, as part of overseeing agencies' implementation of section 208, OMB will rely on the CIO Council to collect information on agencies' initial experience in preparing PIAs, to share experiences, ideas, and promising practices as well as identify any needed revisions to OMB's guidance on PIAs.

VII. Reporting Requirements

Agencies are required to submit an annual report on compliance with this guidance to OMB as part of their annual E-Government Act status report. The first reports are due to OMB by December 15, 2003. All agencies that use information technology systems and conduct electronic information collection activities must complete a report on compliance with this guidance, whether or not they submit budgets to OMB.

Reports must address the following four elements:

A. *Information technology systems or information collections for which PIAs were conducted.* Include the mechanism by which the PIA was made publicly available (website, Federal Register, other), whether the PIA was made publicly available in full, summary form or not at all (if in summary form or not at all, explain), and, if made available in conjunction with an ICR or SOR, the publication date.
B. *Persistent tracking technology uses.* If persistent tracking technology is authorized, include the need that

Case 1:17-cv-01320-CKK Document 35-3 Filed 07/13/17 Page 44 of 110
USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 160 of 265

compels use of the technology, the safeguards instituted to protect the information collected, the agency official approving use of the tracking technology, and the actual privacy policy notification of such use.

C. *Agency achievement of goals for machine readability*: Include goals for and progress toward achieving compatibility of privacy policies with machine-readable privacy protection technology.

D. *Contact information*. Include the individual(s) (name and title) appointed by the head of the Executive Department or agency to serve as the agency's principal contact(s) for information technology/web matters and the individual (name and title) primarily responsible for privacy policies.

Attachment B
E-Government Act of 2002
Pub. L. No. 107-347, Dec. 17, 2002

SEC. 208. PRIVACY PROVISIONS.

A. PURPOSE. — The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

B. PRIVACY IMPACT ASSESSMENTS.—

1. RESPONSIBILITIES OF AGENCIES.—
   a. IN GENERAL.—An agency shall take actions described under subparagraph (b) before—
      i. developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
      ii. initiating a new collection of information that—
         1. will be collected, maintained, or disseminated using information technology; and
         2. includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.
   b. AGENCY ACTIVITIES. —To the extent required under subparagraph (a), each agency shall—
      i. conduct a privacy impact assessment;
      ii. ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and
      iii. if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.
   c. SENSITIVE INFORMATION. —Subparagraph (b)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.
   d. COPY TO DIRECTOR. —Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.
2. CONTENTS OF A PRIVACY IMPACT ASSESSMENT. —
   a. IN GENERAL. —The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.
   b. GUIDANCE. — The guidance shall—
      i. ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and
      ii. require that a privacy impact assessment address—
         1. what information is to be collected;
         2. why the information is being collected;
         3. the intended use of the agency of the information;
         4. with whom the information will be shared;
         5. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
         6. how the information will be secured; and
         7. whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the `Privacy Act').
3. RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—
   a. develop policies and guidelines for agencies on the conduct of privacy impact assessments;
   b. oversee the implementation of the privacy impact assessment process throughout the Government; and
   c. require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

C. PRIVACY PROTECTIONS ON AGENCY WEBSITES. —

1. PRIVACY POLICIES ON WEBSITES. —
   a. GUIDELINES FOR NOTICES. —The Director shall develop guidance for privacy notices on agency websites used by the public.
   b. CONTENTS. —The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—
      i. what information is to be collected;
      ii. why the information is being collected;
      iii. the intended use of the agency of the information;
      iv. with whom the information will be shared;
      v. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
      vi. how the information will be secured; and
      vii. the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the `Privacy Act'), and other laws relevant to the protection of the privacy of an individual.
2. PRIVACY POLICIES IN MACHINE-READABLE FORMATS. — The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

D. DEFINITION. —In this section, the term `identifiable form' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Attachment C

This attachment is a summary by the Federal Trade Commission of its guidance regarding federal agency compliance with the Children's Online Privacy Protection Act (COPPA).

The hallmarks of COPPA for purposes of federal online activity are (i) notice of information collection practices (ii) verifiable parental consent and (iii) access, as generally outlined below:

- Notice of Information Collection Practices

  Agencies whose Internet sites offer a separate children's area and collect personal information from them must post a clear and prominent link to its Internet privacy policy on the home page of the children's area and at each area where it collects personal information from children. The privacy policy should provide the name and contact information of the agency representative required to respond to parental inquiries about the site. Importantly, the privacy policy should inform parents about the kinds of information collected from children, how the information is collected (directly, or through cookies), how the information is used, and procedures for reviewing/deleting the information obtained from children.

  In addition, the privacy policy should inform parents that only the minimum information necessary for participation in the activity is collected from the child.In addition to providing notice by posting a privacy policy, notice of an Internet site's information collection practices must be sent directly to a parent when a site is requesting parental consent to collection personal information from a child. This direct notice should tell parents that the site would like to collect personal information from their child, that their consent is required for this collection, and how consent can be provided. The notice should also contain the information set forth in the site's privacy policy, or provide an explanatory link to the privacy policy.

- Verifiable Parental Consent

  With limited exceptions, agencies must obtain parental consent before collecting any personal information from children under the age of 13. If agencies are using the personal information for their internal use only, they may obtain parental consent through an e-mail message from the parent, as long as they take additional steps to increase the likelihood that the parent has, in fact, provided the consent. For example, agencies might seek confirmation from a parent in a delayed confirmatory e-mail, or confirm the parent's consent by letter or phone call[23].

  However, if agencies disclose the personal information to third parties or the public (through chat rooms or message boards), only the most reliable methods of obtaining consent must be used. These methods include: (i) obtaining a signed form from the parent via postal mail or facsimile, (ii) accepting and verifying a credit card number in connection with a transaction, (iii) taking calls from parents through a toll-free telephone

number staffed by trained personnel, or (iv) email accompanied by digital signature.

Although COPPA anticipates that private sector Internet operators may share collected information with third parties (for marketing or other commercial purposes) and with the public (through chat rooms or message boards), as a general principle, federal agencies collect information from children only for purposes of the immediate online activity or other, disclosed, internal agency use. (Internal agency use of collected information would include release to others who use it solely to provide support for the internal operations of the site or service, including technical support and order fulfillment.) By analogy to COPPA and consistent with the Privacy Act, agencies may not use information collected from children in any manner not initially disclosed and for which explicit parental consent has not been obtained. Agencies' Internet privacy policies should reflect these disclosure and consent principles.

COPPA's implementing regulations include several exceptions to the requirement to obtain advance parental consent where the Internet operator (here, the agency) collects a child's email address for the following purposes: (i) to provide notice and seek consent, (ii) to respond to a one-time request from a child before deleting it, (iii) to respond more than once to a specific request, e.g., for a subscription to a newsletter, as long as the parent is notified of, and has the opportunity to terminate a continuing series of communications, (iv) to protect the safety of a child, so long as the parent is notified and given the opportunity to prevent further use of the information, and (v) to protect the security or liability of the site or to respond to law enforcement if necessary.

Agencies should send a new notice and request for consent to parents any time the agency makes material changes in the collection or use of information to which the parent had previously agreed. Agencies should also make clear to parents that they may revoke their consent, refuse to allow further use or collection of the child's personal information and direct the agency to delete the information at any time.

- Access

At a parent's request, agencies must disclose the general kinds of personal information they collect online from children as well as the specific information collected from a child. Agencies must use reasonable procedures to ensure they are dealing with the child's parent before they provide access to the child's specific information, e.g., obtaining signed hard copy of identification, accepting and verifying a credit card number, taking calls from parents on a toll-free line staffed by trained personnel, email accompanied by digital signature, or email accompanied by a PIN or password obtained through one of the verification methods above.

In adapting the provisions of COPPA to their Internet operations, agencies should consult the FTC's web site at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html or call the COPPA compliance telephone line at (202) 326-3140.

Attachment D

Summary of Modifications to Prior Guidance

This Memorandum modifies prior guidance in the following ways:

* Internet Privacy Policies (Memorandum 99-18):

- must identify when tracking technology is used to personalize the interaction, and explain the purpose of the feature and the visitor's option to decline it.
- must clearly explain when information is maintained and retrieved by personal identifier in a Privacy Act system of records; must provide (or link to) a Privacy Act statement (which may be subsumed within agency's Internet privacy policy) where Privacy Act information is solicited.
- should clearly explain an individual's rights under the Privacy Act if solicited information is to be maintained in a Privacy Act system of records; information about rights under the Privacy Act may be provided in the body of the web privacy policy or via link to the agency's published systems notice and Privacy Act regulation or other summary of rights under the Privacy Act (notice and explanation of rights under other privacy laws should be handled in the same manner).
- when a Privacy Act Statement is not required, must link to the agency's Internet privacy policy explaining the purpose of the collection and use of the information (point-of-collection notice at agency option).

- must clearly explain where the user may consent to the collection or sharing of information and must notify users of any available mechanism to grant consent.
- agencies must undertake to make their Internet privacy policies "readable" by privacy protection technology and report to OMB their progress in that effort.
- must adhere to the regulatory requirements of the Children's Online Privacy Protection Act (COPPA) when collecting information electronically from children under age 13.

*Tracking Technology (Memorandum 00-13):

- prohibition against tracking visitors' Internet use extended to include tracking by any means (previous guidance addressed only "persistent cookies").? authority to waive the prohibition on tracking in appropriate circumstances may be retained by the head of an agency, or may be delegated to (i) senior official(s) reporting directly to the agency head, or to (ii) the heads of sub-agencies.? agencies must report the use of tracking technology to OMB, identifying the circumstances, safeguards and approving official.
- agencies using customizing technology must explain the use, voluntary nature of and the safeguards applicable to the customizing device in the Internet privacy policy.
- agency heads or their designees may approve the use of persistent tracking technology to customize Internet interactions with the government.

* Privacy responsibilities (Memorandum 99-05)

- agencies to identify individuals with day-to-day responsibility for implementing the privacy provisions of the E-Government Act, the Privacy Act and any other applicable statutory privacy regime.
- agencies to report to OMB the identities of senior official(s) primarily responsible for implementing and coordinating information technology/web policies and privacy policies.

---

1. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.
2. Information in identifiable form is defined in section 208(d) of the Act as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Information "permitting the physical or online contacting of a specific individual" (see section 208(b)(1)(A)(ii)(II)) is the same as "information in identifiable form."
3. Clinger-Cohen Act of 1996, 40 U.S.C. 11101(6).
4. Clinger-Cohen Act of 1996, 40 U.S.C. 11103.
5. In addition to these statutorily prescribed activities, the E-Government Act authorizes the Director of OMB to require agencies to conduct PIAs of existing electronic information systems or ongoing collections of information in identifiable form as the Director determines appropriate. (see section 208(b)(3)(C)).
6. Information in identifiable form about government personnel generally is protected by the Privacy Act of 1974. Nevertheless, OMB encourages agencies to conduct PIAs for these systems as appropriate.
7. Consistent with agency requirements under the Federal Information Security Management Act, agencies should: (i) affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured, (ii) acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls, (iii) describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information, and (iv) provide a point of contact for any additional questions from users. Given the potential sensitivity of security-related information, agencies should ensure that the IT security official responsible for the security of the system and its information reviews the language before it is posted.
8. PIAs that comply with the statutory requirements and previous versions of this Memorandum are acceptable for agencies' FY 2005 budget submissions.
9. Section 208(b)(1)(C).
10. See 44 USC Chapter 35 and implementing regulations, 5 CFR Part 1320.8.
11. Item 1 of the Supporting Statement reads: "Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information."
12. Item 2 of the Supporting Statement reads: "Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information

received from the current collection."

13. Item 2 of the Supporting Statement reads: "Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection."
14. Item 10 of the Supporting Statement reads: "Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy."
15. Section 208(c)(1)(B)(v).
16. Section 208(c)(1)(B)(vii).
17. Section 208(c)(1)(B)(i-iv).
18. When multiple Privacy Act Statements are incorporated in a web privacy policy, a point-of-collection link must connect to the Privacy Act Statement pertinent to the particular collection.
19. Attachment C contains a general outline of COPPA's regulatory requirements. Agencies should consult the Federal Trade Commission's COPPA compliance telephone line at (202)-326-3140 or website for additional information at: http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.
20. Consistent with current practice, the agency head or designee may limit, as appropriate, notice and reporting of tracking activities that the agency has properly approved and which are used for authorized law enforcement, national security and/or homeland security purposes.
21. Section 208(c)(1)(B)(vi).
22. Federal Information Security Management Act of 2002 (Title III of P.L. 107-347), OMB's related security guidance and policies (Appendix III to OMB Circular A-130, "Security of Federal Automated Information Resources") and standards and guidelines development by the National Institute of Standards and Technologies.
23. This standard was set to expire in April 2002, at which time the most verifiable methods of obtaining consent would have been required; however, in a Notice of Proposed Rulemaking, published in the Federal Register on October 31, 2001, the FTC has proposed that this standard be extended until April 2004. 66 Fed. Reg. 54963.

FILED
2010 Apr-21 PM 03:1
U.S. DISTRICT COUR
N.D. OF ALABAM

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

JIM HENRY PERKINS and JESSIE FRANK QUALLS, on their own behalf and on the behalf of all others similarly situated,

Plaintiffs,

v. **CV No. 2:07-310-IPJ**

UNITED STATES DEPARTMENT OF VETERANS AFFAIRS; et al.

Defendants.

MEMORANDUM OPINION

This case is before the court upon remand from the Eleventh Circuit to conduct a "claim-by-claim" analysis to determine the validity of plaintiffs' remaining challenges brought under the Administrative Procedures Act ("APA"), 5 U.S.C. § 551 *et seq.*, and seeking to enforce provisions of the Privacy Act, 5 U.S.C. § 552a; the E-Government Act of 2002, 44 U.S.C. § 3501 note; and the Veterans Benefits, Health Care, and Information Technology Act of 2006, 38 U.S.C. § 5724. Only counts two, five, six, and eight remain, and the court examines each claim in turn.

Factual Background

On January 22, 2007, an employee of the U.S. Department of Veterans

Affairs ("VA") reported an external hard drive containing personally identifiable information and individually identifiable health information of over 250,000 veterans was missing from the Birmingham, Alabama Medical Center's Research Enhancement Award Program ("REAP"). VA Office of Inspector General ("OIG") Report, at 7. The IT Specialist responsible for the external hard drive, "John Doe," used the hard drive to back up data on his computer and other data from a shared network drive.[1] The hard drive is thought to contain the names, addresses, social security numbers ("SSN"), dates of birth, phone numbers, and medical files of hundreds of thousands of veterans and also information on more than 1.3 million medical providers. VA OIG Report at 7, 9 (doc. 33-2). To date, it has not been recovered.

John Doe was an IT Specialist working for the Birmingham REAP, a program that focused on "changing the practices of health care providers to ensure that they provide the latest evidence-based treatment, and on using VA databases

---

[1]The REAP Director approved the purchase of external hard drives as a means to provide more space to the Medical Center's near-full server. VA OIG Report, at 15. No policy required the protection of sensitive data on removable computer storage devices unless such devices were to be carried outside a VA facility. *Id.* at 16. The REAP Director claimed the Information Security Officer ("ISO") conferred with him in making the decision to purchase the external hard drives, but the ISO claimed he was not involved and did not know of the need for additional server space. The VA OIG concluded no one made a timely request to the ISO for additional space. VA OIG Report, at 15.

to link the care of VA patients to more general information on the population as a whole." *Id.* at 3. To reach these goals, the Birmingham REAP collects data on patients and medical providers from multiple sources for dozens of separate research projects." *Id.* The Data Unit of the Birmingham REAP was comprised of the Data Unit Manager, three IT Specialists, and two student program support Assistants. *Id.* at 4. John Doe worked "with national VA databases and design[ed] statistical programs to support Birmingham REAP research projects." *Id.*

The VA OIG identified three projects for which John Doe was conducting research. The first "involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medication to improve glucose levels, cholesterol, and blood pressure"; the second "involved examining the quality of care to patients following myocardial infarction . . ., and attempted to determine whether certain demographic characteristics of the medical providers, such as their age, impacted the care rendered to these patients"; and the third "involved using a patient survey to identify use of over-the-counter medications in patients taking prescription medications and link the information obtained to various VA databases to determine whether patients suffered any adverse effects from the combination of medications." *Id.* at 22, 25, 30. In gathering the information needed to complete these projects, John Doe improperly received

access to various databases and stores of information, and various components of the VA improperly released information to John Doe or gave John Doe such access. *Id.* at 22-33. He was therefore able "to accumulate and store vast amounts of individually identifiable health information that was beyond the scope of the projects he was working on. [The OIG] believe[s] much of this information was stored on the missing external hard drive." *Id.* at 22. Accurate reporting of what information was on the external hard drive has been difficult because the hard drive is still missing; John Doe encrypted or deleted multiple files from his computer after reporting the data missing; and John Doe was not initially forthright with criminal investigators. *Id.* at ii.

After John Doe reported the missing hard drive on January 22, 2007, the VA Security Operations Center ("SOC") was immediately notified. *Id.* at 7. The SOC wrote a report and provided it to the VA OIG on January 23, 2007; on that same day, an OIG criminal investigator came to the Birmingham VAMC and conducted an interview. The Federal Bureau of Investigation became involved in the investigation on January 24, 2007. A forensic analysis of John Doe's computer began on January 29, 2007, and on February 1, 2007, the OIG began to analyze what data could have been on the missing hard drive. *Id.* at 8, 9. Press releases dated on February 2 and 10, 2007, discussed the loss of the hard drive and the information it contained.

> Subsequent to the reported loss of the Birmingham REAP data but prior to receiving the results of the OIG analysis of this data on February 7, 2007, VA senior management concluded that anyone whose SSN was thought to be contained in any of the missing files, irrespective of the ability of anyone possessing this data to match an SSN with a name or any other personal identifier, should be notified and offered credit protection. The basis for this decision was a memorandum issued on November 7, 2006. . . . The memorandum states that "in the event of a data loss involving individual and personal information. . . VA officials have a responsibility to notify the individual(s) of the loss in a timely manner and to offer these protection services."

Id. at 11. The VA sent letters to those individuals whose information was thought to be compromised by the data breach, which gave them the option of one year of free credit monitoring services. *Id.* at 12.

The VA had also requested the Department of Health and Human Services to perform a risk analysis focusing on the Centers for Medicaid and Medicare Services ("CMS") data involved in the breach. *Id.* The missing external hard drive contained approximately 1.3 million health care providers' information,

including the SSNs of 664,165 health care providers. *Id.* On March 28, 2007, the CMS Chief Information Officer and Director sent a letter to the VA Assistant Secretary for Office of Information and Technology that stated, based on the CMS's completed independent risk analysis:

> [T]here is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned. The letter requested that "VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file."

Id. From April 17 to May 22, 2007, the VA sent notification letters to the 1.3 million health care providers. *Id.* By May 31, 2007, it sent additional letters offering one year of credit monitoring to the 664,165 health care providers whose SSNs appeared to be on the hard drive. VA OIG Report, at 12.

Analysis

A valid claim under the APA must attack agency action, which is defined as "includ[ing] the whole or a part of an agency rule, order, license, sanction, relief or the equivalent or denial thereof, or failure to act." *Fanin v. U.S. Dep't of*

Veterans Aff., 572 F.3d 868, 877 (11th Cir. 2009) (citing 5 U.S.C. § 551(13)).

> If the claim attacks an agency's action, instead of failure to act, and the statute allegedly violated does not provide a private right of action, then the "agency action" must also be a "final agency action." [5 U.S.C. § 704; *see also Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 61-62, 124 S.Ct. 2373, 2379 (2004)]. "To be considered 'final,' an agency's action: (1) must mark the consummation of the agency's decisionmaking process–it must not be of a merely tentative or interlocutory nature; and (2) must be one by which rights or obligations have been determined, or from which legal consequences will flow. *U.S. Steel Corp. v. Astrue*, 495 F.3d 1272, 1280 (11th Cir. 2007)(quoting *Bennett v. Spear*, 520 U.S. 154, 177-78, 117 S.Ct. 1154, 1168 (1997)).

Id. However, if the claim challenges a failure to act, the court may compel "agency action unlawfully withheld or unreasonably delayed. . . only where a plaintiff asserts that an agency failed to take a *discrete* agency action that it is *required* to take." *Id.* at 877-878 (citing *Norton*, 542 U.S. at 64) (emphasis in original).

Further, the court notes the remaining claims seek only injunctive and

declaratory relief. Such relief may be granted only if the plaintiffs demonstrate that they are "likely to suffer future injury." *City of Los Angeles v. Lyons*, 461 U.S. 95, 105, 103 S.Ct. 1660, 1667 (1983); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564, 112 S.Ct. 2130, 2138 (1992) (citing *Lyons*, 461 U.S. at 102) ("'Past exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief.'"); *Seigel v. LePore*, 234 F.3d 1163, 1176-77 (11th Cir. 2000) (*en banc*) ("As we have emphasized on many occasions, the asserted irreparable injury "must be neither remote nor speculative, but actual and imminent.") (citations omitted). *Emory v. Peeler*, 756 F.2d 1547, 1552 (11th Cir. 1985) (To grant declaratory relief, "there must be a substantial continuing controversy between parties having adverse legal interests. The plaintiff must allege facts from which the continuation of the dispute may be reasonably inferred. Additionally, the continuing controversy . . . must be real and immediate, and create a definite, rather than speculative threat of future injury.").

Count Two

The plaintiffs claim that the VA failed "to create and maintain an accounting of the date, nature, and purpose of its disclosures" pursuant to the Privacy Act, 5 U.S.C. § 552a(c)(1), when John Doe accessed VA files to complete

VA projects. Joint Status Report ("JSR"), at 8 (doc. 56). The Privacy Act requires

> [e]ach agency, with respect to each system of records under its control, shall–
>
> (1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of–
>
> (A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and
>
> (B) the name and address of the person or agency to whom the disclosure is made. . .

5 U.S.C. § 552a(c)(1). Under the exception provided in subsection (b)(1), agencies need not provide an accounting for disclosures made to "officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). Accordingly, to the extent John Doe needed the information that he accessed to perform his duties, the VA had no obligation to account.

To the extent John Doe had no need for the information contained on the external hard drive in the performance of his duties, the plaintiffs must show the disclosure was pursuant to one of the provisions in 5 U.S.C. § 552a(b)(3)-(12).

See 5 U.S.C. § 552a(c)(1)(A). After failing to argue in the JSR that any of those subsections apply, plaintiffs now claim that the VA's disclosure to John Doe falls under 5 U.S.C. § 552a(b)(5), which requires accounting when the disclosure is "to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable."

However, the accounting requirement in 5 U.S.C. § 552a(b)(5) is not triggered by the activity at issue in this case. An accounting is required only upon a disclosure to a recipient described in that subsection. Although "recipient" is not defined in the Privacy Act, it does not stand to reason that an agency that maintains records needed by one of its own researchers to fulfill his duties would be required to provide *itself* with "advance adequate written assurance that the record will be used solely as a statistical research or reporting record." Indeed, pertinent legislative history and Office of Management and Budget ("OMB") regulations suggest that an accounting was only intended when the disclosures were to individuals or agencies outside the agency maintaining the record. *See* S. REP. NO. 93-1183 (1974) *reprinted in* U.S. CODE CONGRESSIONAL AND ADMINISTRATIVE NEWS, 6916, 6967 (stating that subsection 201(b)(4) "[r]equires any federal agency that maintains a personal information system or file to maintain an accurate accounting of the date, nature, and purpose of nonregular access

granted to the system, and each disclosure of personal information made to any person *outside the agency, or to another agency. . . .*") (emphasis added); H.R. No. 93-1416, 2 (describing the summary and purpose of the Act as "requir[ing] agencies to keep an accounting of transfers of personal records *to other agencies and outsiders*"); 40 Fed. Reg. 28955 (July 9, 1975) (differentiating between "agencies disclosing records" and "recipient agencies" in the context of 5 U.S.C. § 552a(b)(5)).

Even if subsection (b)(5) is applicable in this case, the plaintiffs argue only that John Doe gave an advance adequate written assurance before accessing information from only one database, the Veterans Integrated Service Network ("VISN") 7 Data Warehouse. Plaintiff's Response (doc. 64) at 4. Accordingly, subsection (b)(5) applies only for John Doe's access to the VISN 7 Data Warehouse to perform research for "Project 1," which involved diabetes management research. *See* VA OIG Report, at 22. Moreover, the plaintiffs cannot show that any failure to account for John Doe's access to the VISN 7 Data Warehouse to research diabetes management is causing them harm. Although the plaintiffs are upset about the loss of their personal information and the prospect of potential credit fraud in the future, any accompanying harm is attributable to the

loss of the information in the first place, *not* the purported failure to account.[2] Thus, even assuming *arguendo* that 5 U.S.C. § 552a(b)(5) applies, the plaintiffs cannot show that the alleged harm is fairly traceable to the VA's conduct, a deficiency fatal to their claim. *See Allen v. Wright*, 468 U.S. 737, 753 & n.19, 104 S.Ct. 3315, 3325 & n.19 (1984) (plaintiffs do not have standing where they failed to allege injuries that are caused by the defendants).

Because of these sufficient and independent reasons, the plaintiffs have not shown that the VA failed to take discrete agency action that it was required to take. Accordingly, the court finds that the plaintiffs have failed to state a claim upon which relief can be granted, and Count Two is due to be **DISMISSED**.

---

[2]The plaintiffs urge, "The Veterans have a right to know what information [was on the hard drive]. They deserve to know the 'purpose' for which John Doe was using the information," Plaintiff's Response, at 8 (doc. 64). However, the VA OIG report details, to the extent determinable, the information on the hard drive and the purpose for which John Doe was accessing the information. The VA OIG Report states that the hard drive is believed to contain "personally identifiable information and/or individually identifiable health information for over 250,000 veterans, and information obtained from the [CMS], on over 1.3 million medical providers." VA OIG Report, at i. Moreover, it was difficult for the VA to make such a determination, as John Doe was not candid when he was interviewed; he deleted or encrypted files from his computer after the hard drive went missing; and he tried to hide the extent, magnitude, and impact of the missing data. *Id.* at ii. Lastly, the plaintiffs know that the purpose John Doe was accessing the VISN 7 Data Warehouse was related to his research for "Project 1," *id.* at 22-23, which "involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medication to improve glucose levels, cholesterol, and blood pressure," VA OIG Report, at 22.

Count Five

Count Five involves the VA's alleged failure to establish appropriate safeguards in violation of the Privacy Act, 5 U.S.C. § 552a(e)(10). The plaintiffs have failed to argue that the alleged conduct of the VA constituted a failure of discrete agency action that the VA was required to take, but request that Count Five "move forward as detailed in the Plaintiffs' Statement in the Joint Report." Plaintiff's Brief, at 13 (doc. 64). In the Joint Status Report, the plaintiffs devote just over one page to briefing this issue and cite 5 U.S.C. § 552a(e)(10),[3] arguing that the VA failed to enforce this subsection in the numerous ways listed in their complaint.[4] Joint Status Report ("JSR"), at 10-11 (doc. 56). The plaintiffs then

---

[3]5 U.S.C. § 552a(e)(10) requires the VA to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

[4]Plaintiffs cite specifically to paragraph 80 of the Second Amended Complaint (doc. 21), which states:

> Among other things, Defendants' failures include operating a computer system or database from which an employee, including John Doe, can download or copy information, like the Personal Information and the Medical Information, onto the VA External Hard Drive without proper encryption and when not necessary to perform his or her duties; failing to conduct a data access inventory for John Doe and other VA employees and contractors with access to the VA's office at the Pickwick Conference Center; failing to provide software that would require or enable encryption of data downloaded or copied

ask the court for an injunction forcing full implementation and compliance "with Handbook 6500 and other procedures and policies put in place in Birmingham by the VA in response to this incident, to conduct an independent audit of its compliance, and to file that audit with the court." Plaintiff's Response, at 14 (doc. 64) (footnotes added). Such an injunction is untenable.

Handbook 6500 is a seventy-one page (seven appendices excluded) document that details the responsibilities of almost two dozen information security personnel and dozens of policies and procedures. As pointed out by the defense, policies explained in the Handbook include maintaining the temperature in the building and proper use of the facsimile machines. In addition, the "other procedures and policies" put in place at the Birmingham facility are also

---

> to mobile hard drives and devices, like the VA External Hard Drive from VA computers and databases at the VA offices and facilities in the Birmingham, Alabama area; failing to secure the VA External Hard Drive under lock and key when not in the immediate vicinity of John Doe; failing to house and protect the VA External Hard Drive to reduce the opportunities for unauthorized access, use, or removal; failing to provide intrusion detection systems at the VA office at the Pickwick Conference Center; failing to store the VA External Hard Drive in a secure area that requires proper escorting for access; failing to require and conduct appropriate background checks on all VA employees and contractors with access to the VA Office in the Pickwick Conference Center; and failing to protect against the alienation and relinquishment of control over the VA External Hard Drive, causing the Personal Information and Medical Information to be exposed to unidentified third parties.

Second Amended Complaint (doc. 21), ¶ 80.

numerous. *See e.g.*, VA Directive 6504 (doc. 61-3) (governing the transmission, transportation and use of, and access to, VA data outside VA facilities); VA Handbook 6500, at 7 (doc. 61-4) (a seventy-one page document "establish[ing] the foundation for VA's comprehensive information security program and its practices that will protect the confidentiality, integrity, and availability of information"); Medical Center Memo 00-ISO-02 (doc. 61-5) ("assign[ing] responsibility and establish[ing] procedures for managing computer files at the Birmingham VA Medical Center"); Medical Center Memo 00-ISO-05 (doc. 61-6) (requiring VA employees at the Medical Center to get permission before use of removable storage media, especially Universal Serial Bus ("USB") devices, and requiring written permission for the removal of sensitive information from VA facilities); Information Security Program VISN 7 AIS Operational Security Policy (doc. 61-9) (establishing procedures to implement a "structured program to safeguard all IT assets"); Memorandum 10N7-077 of VISN 7 VA Southeast Network (doc. 61-10) (stating "It is the policy of VISN 7 that no sensitive information ([personal health information or personal identifiable information]) will be stored on the storage media of any device without encryption or where the device is not *physically secured* to prevent accidental loss of sensitive information in the event of theft") (emphasis in original).

Cases that suggest a broad injunction enforcing all of these policies is

appropriate are "relic[s] of a time when the federal judiciary thought that structural injunctions taking control of executive functions were sensible. That time has past." *Rahman v. Chertoff*, 530 F.3d 622, 626 (7th Cir. 2008). "The limitation to discrete agency action precludes the kind of broad programmatic attack [the Supreme Court] rejected in *Lujan v. National Wildlife Federation*, 497 U.S. 871, 110 S.Ct 3177, 111 L.Ed.2d 695 (1990)." *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 64, 124 S.Ct. 2373, 2379-2380 (2004); *see Lujan*, 497 U.S. at 891 When presented with similar circumstances in *Lujan*, the Supreme Court responded:

> Respondent alleges that violation of the law is rampant within this program-failure to revise land plans in proper fashion, failure to submit certain recommendations to Congress, failure to consider multiple use, inordinate focus upon mineral exploitation, failure to provide required public notice, failure to provide adequate environmental impact statements. Perhaps so. But respondent cannot seek *wholesale* improvement of this program by court decree, rather than in the office of the Department or the halls of Congress, where programmatic improvements are normally made.

Lujan, 497 U.S. at 891. Courts are not empowered to compel "compliance with

broad statutory mandates," *Norton*, 542 U.S. at 66-67, nor can they engage in general review of an agency's day-to-day operations to ensure such compliance. *Id.*; *Lujan*, 497 U.S. at 899.

Even if this court could pass on such a generalized challenge, the court is convinced that Count Five is moot.

> "'[A] case is moot when the issues presented are no longer "live" or the parties lack a legally cognizable interest in the outcome.' " *County of Los Angeles v. Davis,* 440 U.S. 625, 631, 99 S.Ct. 1379, 59 L.Ed.2d 642 (1979) (quoting *Powell v. McCormack,* 395 U.S. 486, 496, 89 S.Ct. 1944, 23 L.Ed.2d 491 (1969)). The underlying concern is that, when the challenged conduct ceases such that " 'there is no reasonable expectation that the wrong will be repeated,' " *United States v. W.T. Grant Co.,* 345 U.S. 629, 633, 73 S.Ct. 894, 97 L.Ed. 1303 (1953), then it becomes impossible for the court to grant " 'any effectual relief whatever' to [the] prevailing party," *Church of Scientology of Cal. v. United States,* 506 U.S. 9, 12, 113 S.Ct. 447, 121 L.Ed.2d 313 (1992) (quoting *Mills v. Green,* 159 U.S. 651, 653, 16 S.Ct. 132, 40 L.Ed. 293 (1895)).

City of Erie v. Pap's A.M., 529 U.S. 277, 287, 120 S.Ct. 1382, 1390 (2000).

Because the evidence submitted to the court shows that new security procedures and policies have been implemented and the deficiencies revealed in the VA OIG Report have been remedied, there is no "live" issue for which this court can grant effectual relief.

Count Six

In Count Six, the plaintiffs claim that the VA failed to perform a privacy impact assessment ("PIA") pursuant to the E-Government Act of 2002 when it procured the external hard drives. Pursuant to the E-Government Act, agencies must perform a PIA before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form." 44 U.S.C. § 3501 note (E-Government Act of 2002, § 208(b)(1)(A)). The definition of "information technology" includes "any equipment or interconnected system . . . used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly . . . ." 40 U.S.C. § 11101(6); *see* 44 U.S.C. § 3501 note, § 201 (applying definitions from 44 U.S.C. §§ 3502, 3601); 44 US.C. § 3502(9) (applying the definition of 40 U.S.C. § 11101(6)). The disputed issue is whether the purchase of the external hard drives triggered the duty to perform a PIA.

The plaintiffs claim that the inclusion of "any equipment" in the definition of information technology brings the hard drives within the meaning of the term, thereby requiring the PIA. However, such an interpretation is implausible, as it would require government agencies that maintain personal information on individuals to conduct or update a PIA each time it purchases any computer, monitor, router, telephone, calculator, or other piece of equipment involved in a system that stores, analyzes, or manages the data. Rather, the purchase of several external hard drives, seems to be a "minor change[] to a system or collection that do[es] not create new privacy risks," and therefore does not require a PIA. *See* M-03-22, Attachment A 2.B.3.g., Office and Management and Budget ("OMB") Guidance Implementing the Privacy Provisions of the E-Government Act of 2002, at Section II.B.3.f (doc. 61-15) (hereinafter "M-03-22").

Lending support to this interpretation is the fact that PIAs are required to address (1) what information is collected and why, (2) the agency's intended use of the information, (3) with whom the information would be shared, (4) what opportunities the veterans would have to decline to provide information or to decline to share the information, (5) how the information would be secured, and (6) whether a system of records is being created. *See* 44 U.S.C. § 3501 note (E-Government Act of 2002, § 208(b)(2)(B)); M-03-22, at Section II.C.1.a. These types of inquiries are certainly appropriate and required when the VA initially

created the Birmingham VAMC system and began collecting data, but not where already collected and stored data is simply being transferred from a server to an external hard drive. The factors above are not relevant for such a transfer and a new PIA would not be informative of what information is being collected, the intended use of the information, or with whom the information would be shared. Under such circumstances, Congress surely did not intend a PIA to be performed.

To the extent the plaintiffs argue that security procedures were not followed or hardware security protocols were breached at the VA facility in Birmingham when the external hard drive went missing, such claims are not actionable under the E-Government Act of 2002. Rather, those arguments should have been pursued pursuant to the Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541 *et seq.*, a claim that the plaintiffs waived after not pursuing it on appeal. *Fanin v. U.S. Dep't of Veterans Affairs*, 572 F.3d 868, 876 n.1.

Count 8

The final count before the court involves the VA's alleged failure to perform an independent risk analysis ("IRA") to determine the risk presented by the loss of the hard drive pursuant to the Veterans Benefits, Health Care, and Information Technology Act of 2006 (VBHCITA), 38 U.S.C. § 5724(a)(1). The plaintiffs also claim that the VA acted unreasonably by providing only one year of credit monitoring services.

The VBHCITA[5] provides:

> In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall ensure that, as soon as possible after the data breach, a non-Department entity or the Office of Inspector General of the Department conducts an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.

38 U.S.C. § 5724(a)(1).

After John Doe reported the missing hard drive on January 22, 2007, the VA launched an immediate investigation that culminated in the decision to offer one year of free credit monitoring services for 198,760 living individuals whose information was contained on the hard drive. VA OIG Report, at 12. The VA made this decision *before* the completion of the IRA conducted by the Centers for Medicaid & Medicare Services ("CMS"). On February 7, 2007, VA senior

---

[5]The VBHCITA became effective December 22, 2006. The data breach incident at issue occurred on January 22, 2007. The VA passed regulations that became effective June 22, 2007, six months after the passage of the VBHCITA and five months after the loss of the external hard drive.

management decided that anyone whose SSN was on the hard drive should be notified and offered credit protection. *Id.* at 11. Approximately one and one-half months later, on March 28, 2007, the CMS Chief Information Officer and Director stated that based on the IRA, "There is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned." *Id.* at 12. He recommended that the "VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file." *Id.* Notification letters were sent out to the health care providers by May 31, 2007. *Id.*

Thus, the VA proactively assumed that the veterans were at risk and provided the remedy provided in the statute[6] *before* it had confirmation from the IRA that such a remedy was appropriate under the circumstances. By presuming a reasonable risk of harm from the disclosure of personally identifiable information and providing credit protection services required when an IRA reveals a "reasonable risk" of harm, *see* 38 U.S.C. § 5724(a)(2), the VA has provided the

---

[6]In addition, VA regulations limit credit monitoring awarded to those who are subject to a reasonable risk for misuse of sensitive personal information to one year. 38 C.F.R. § 75.118(a).

plaintiffs with any relief they are due.[7] Indeed, the IRA conducted by CMS affirmed the propriety of the relief offered by the VA.

Despite having been given such relief, the plaintiffs insist the IRA was insufficient and urge an additional IRA focusing on the veterans must be completed. However, the statute does not require an *individual* risk analysis as the plaintiffs state in their JSR, *See* JSR, at 12-13, 15, only an *independent* risk analysis.[8] The VA OIG Report contains multiple groups of individuals whose private information was compromised: veterans, VA OIG Report, at 7; physicians, *id.* at 10; deceased physicians, *id.*; other health care providers, *id.*; non-veteran, non-VA employees, *id.* at 24; and VA employees, *id.* Furthermore, some veterans were only identified by their SSNs; others were identified by SSNs and dates of birth; others by their name, SSN, and medical information; and others identified

---

[7] The plaintiffs offer a General Accountability Office report that states that a May 5, 2006, incident involving a missing tape with sensitive information of thousands of individuals on it warranted "credit protection and data breach analysis for 2 years." JSR, at 14. As the plaintiffs explain, however, only one year of credit protection was offered, while two years of breach analysis was given. Declaration of Michael Hogan ("Hogan Decl."), ¶¶ 2 (doc. 61-19) and Attachment A (doc. 61-20).

[8]The plaintiffs' argument that the CMS was an inappropriate entity to perform the IRA has no merit, as the statute requires either the VA OIG or a non-Department [of Veterans Affairs] entity to conduct the IRA. 38 U.S.C. § 5724(a)(1). The CMS is under the purview of the Department of Health and Human Services.

by various combinations of seven fields of identifying information. *Id.* at 9. The health care providers are identified on the hard drive by different combinations of forty-eight different fields of data. *Id.* at 10. All of this information was on a single external hard drive lost during a single data breach. The statute only requires an "independent risk analysis of the data breach," not multiple IRAs for each group of individuals whose information was compromised. *See* 38 U.S.C. § 5724(a)(1).

Because the plaintiffs were awarded appropriate relief and because the VA conducted an adequate IRA of the data breach, the court finds that the VA did not fail to take agency action it was required to take with respect to count eight.

Conclusion

Having considered the foregoing and being of the opinion that the plaintiffs have failed to properly state any claims challenging final agency action under the Administrative Procedures Act, 5 U.S.C. § 551 *et seq.*, the court finds that Counts Two, Five, Six, and Eight shall be **DISMISSED**. The court shall so rule by separate order.

DONE and **ORDERED**, this the 21st day of April 2010.

INGE PRYTZ JOHNSON
U.S. DISTRICT JUDGE

USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 189 of 265

Interstate Voter Registration Crosscheck Program

18-F-1517//0789

JA000185

National Association of State Election Directors

January 26, 2013

Kris W. Kobach

National Voter Registration Act of 1993

Page 190 of 285
Filed: 08/18/2017
Document #1689466
USCA Case #17-5171
18-F-1517//0790
JA000186

- **Section 2 Findings and Purposes**
- (b) Purposes
- (1) to establish procedures that will increase the number of eligible citizens who register to vote in elections for Federal office;
- (2) to make it possible for Federal, State, and local governments to implement this subchapter in a manner that enhances the participation of eligible citizens as voters in elections for Federal office;
- (3) to protect the integrity of the electoral process; and
- **(4) to ensure that accurate and current voter registration rolls are maintained.**

USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 191 of 265

From the Federal Election Commission's guide: Implementing the National Voter Registration Act of 1993:

The features (of the National Voter Registration Act) include a requirement that states "conduct a general program" the purpose of which is "to protect the integrity of the electoral process by ensuring the maintenance of an accurate and current voter registration roll for elections for Federal office"

18-F-1517//0791

JA000187

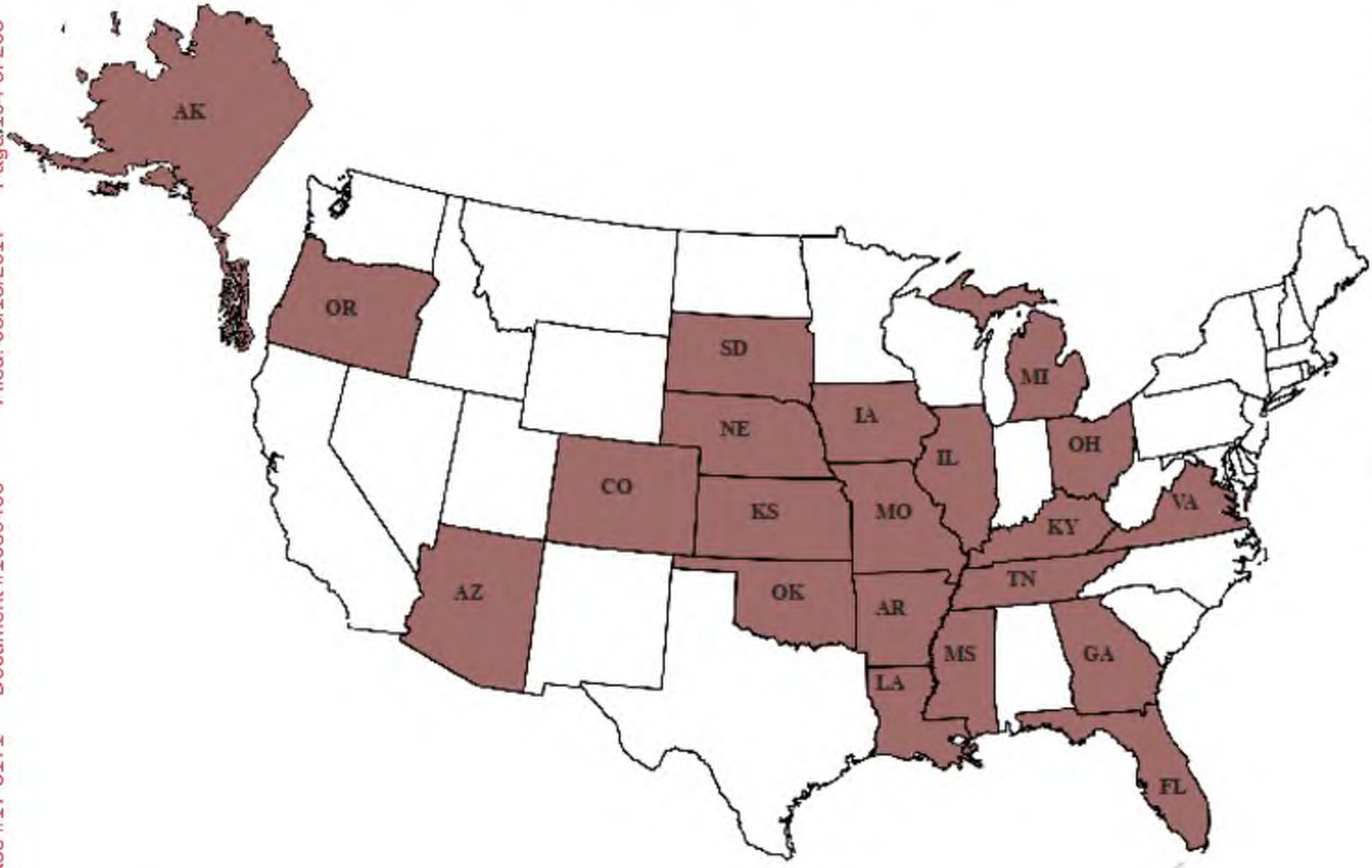
Participants in 2005

Participants in 2012

USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 194 of 265

18-F-1517//0794

JA000190



2013 Interstate Crosscheck

Participating states as of Jan. 10, 2013

2012 Crosscheck Program—Number of Records Compared

Arizona	3,545,891	Michigan	7,337,846
Arkansas	1,528,458	Mississippi	2,002,406
Colorado	3,375,891	Missouri	4,069,576
Illinois	8,248,736	Nebraska	1,129,943
Iowa	2,113,199	Oklahoma	2,000,767
Kansas	1,702,495	South Dakota	560,147
Kentucky	1,303,684	Tennessee	3,468,503
Louisiana	2,860,281		

Total Records: 45,247,823

USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 195 of 265
18-F-1517//0795
JA000191

Interstate Crosscheck Data Format

Field	Format	Example
Status	A=Active; I=Inactive	A
Date_Generated	YYYY/MM/DD	2010/01/01
First_Name		Bob
Middle_Name		Alan
Last_Name		Jones
Suffix Name		Jr
Date_of_Birth	YYYY/MM/DD	1940/06/16
Voter_ID_Number		123456
Last_4_SSN		7890
Mailing Address	Line 1 Line 2 City State Zip	123 Anywhere St...
County		Allen
Date_of_Registration	YYYY/MM/DD	1970/01/01
Voted_in_2010	Y=did vote; N=did not vote	Y

USCA Case #17-5171 Document #1689460 Filed: 09/18/2017 Page 135 of 285

18-F-1517//0796

JA000192

Kris W. Kobach

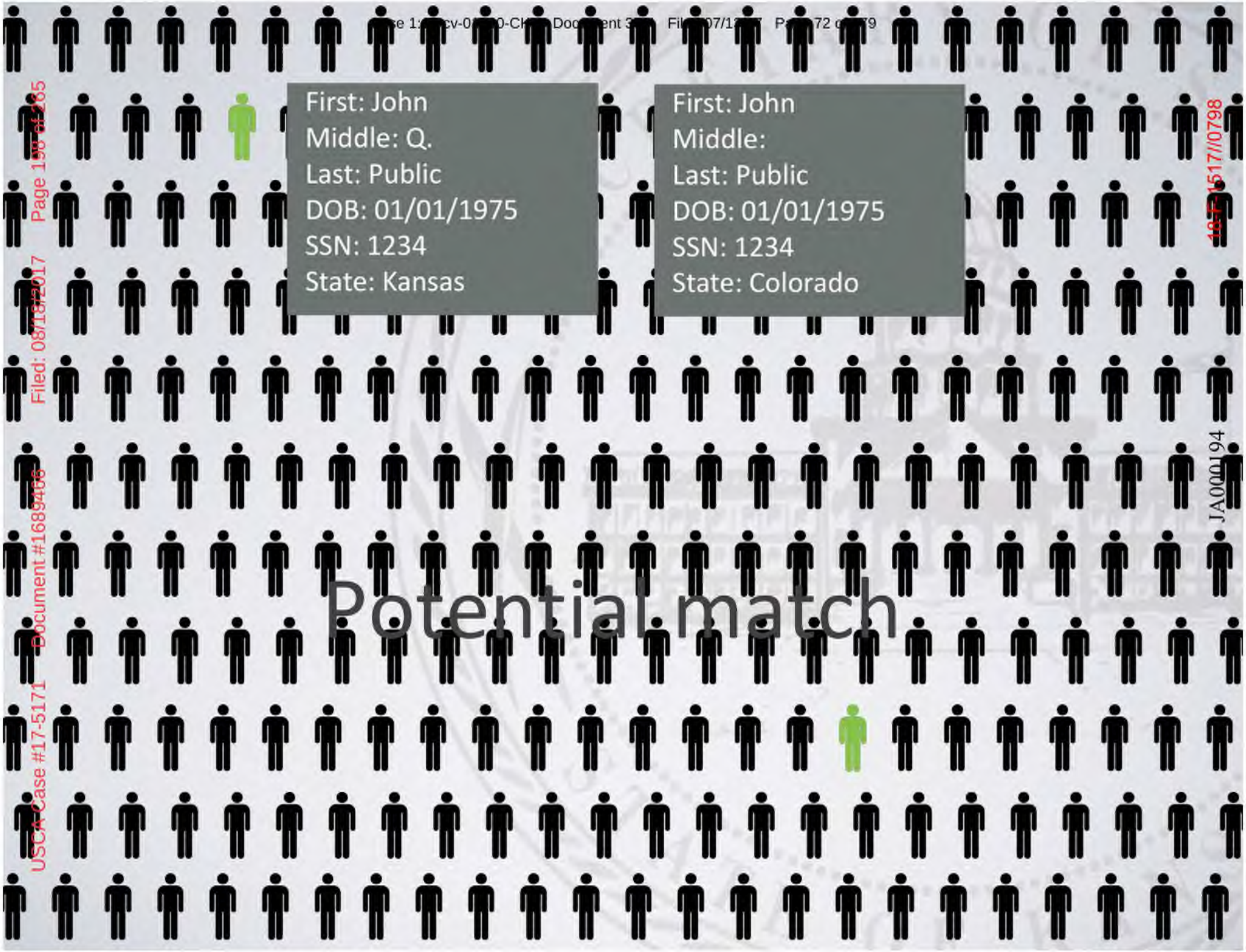
How does it work?

- Each state pulls data on January 15 each year using prescribed data format
- Upload data to secure FTP site (hosted by Arkansas)
- Kansas IT department pulls data, runs comparison, uploads results to FTP site
- Each state downloads results from FTP site, processes them according to state laws & regulations
- Kansas deletes all other states' data

USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 197 of 285

18-F-1517//0797

JA000193



USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 198 of 265
18-7517//0798
JA000194

Grid of Potential Duplicate Voters Within States

by DOB Last Name First Name

2022	AZ	AR	CO	IL	IA	KS	KY	LA	MI	MS	MO	NE	OK	SD	TN
AZ		2,829	24,863	16,014	7,153	3,687	688	2,062	27,617	2,220	7,569	3,306	4,006	2,449	3,614
AR	2,829		4,557	6,950	2,430	2,686	691	5,957	5,085	6,477	11,049	995	7,403	433	7,180
CO	24,863	4,557		19,902	10,850	10,035	1,054	5,065	17,086	3,309	12,498	8,927	8,306	3,937	6,153
IL	16,014	6,950	19,902		31,882	6,311	2,467	5,207	49,260	10,766	39,658	3,803	4,834	1,500	12,469
IA	7,153	2,430	10,850	31,882		4,706	526	1,558	7,019	1,797	11,563	10,954	2,031	4,865	2,806
KS	3,687	2,686	10,035	6,311	4,706		401	1,369	4,461	1,397	31,082	4,196	6,575	905	2,205
KY	688	691	1,054	2,467	526	401		873	2,267	1,085	1,195	233	576	117	1,905
LA	2,062	5,957	5,065	5,207	1,558	1,369	873		6,851	17,744	5,254	810	2,829	277	4,422
MI	27,617	5,085	17,086	49,260	7,019	4,461	2,267	6,851		7,527	12,960	2,416	4,067	1,265	16,956
MS	2,220	6,477	3,309	10,766	1,797	1,397	1,085	17,744	7,527		5,607	780	2,364	305	21,661
MO	7,569	11,049	12,498	39,658	11,563	31,082	1,195	5,254	12,960	5,607		4,244	7,539	1,300	7,804
NE	3,306	995	8,927	3,803	10,954	4,196	233	810	2,416	780	4,244		1,126	2,608	1,108
OK	4,006	7,403	8,306	4,834	2,031	6,575	576	2,829	4,067	2,364	7,539	1,126		402	2,858
SD	2,449	433	3,937	1,500	4,865	905	117	277	1,265	305	1,300	2,608	402		537
TN	3,614	7,180	6,153	12,469	2,806	2,205	1,905	4,422	16,956	21,661	7,804	1,108	2,858	537	
Totals	108,077	64,722	136,542	211,023	100,140	80,016	14,078	60,278	164,837	83,039	159,322	45,506	54,916	20,900	91,67

USCA Case #17-5105 Document #1689466 Filed: 08/18/2017 Page 150 of 165

18-5105//0799

Success in Kansas

Double Votes from 2008 and 2010 Referred to Prosecution Discovered through Interstate Crosscheck Program	
2008	**2010**
Kansas - Kentucky	Kansas – Arkansas (2)
Kansas - Colorado	Kansas – Colorado (5)
Kansas - Kansas	Kansas – Iowa
	Kansas – Louisiana
	Kansas – Nebraska
	Kansas - Oklahoma

USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 200 of 265

18-F-1517//0800

JA000196

Filed: 08/18/2017 Page 201 of 265 USCA Case #17-5171 Document #1689466

Success in other states - Colorado

- Four individuals indicted for voting in Colorado and Arizona in first year of participation
- Six additional cases of double voting referred to FBI in 2012

STATE OF COLORADO
Department of State
1700 Broadway
Suite 250
Denver, CO 80290

Scott Gessler
Secretary of State

William A. Hobbs
Deputy Secretary of State

FOR IMMEDIATE RELEASE
January 23, 2012

News Release

MEDIA CONTACTS: Rich Coolidge
richard.coolidge@sos.state.co.us
Andrew Cole
andrew.cole@sos.state.co.us
(303) 860-6903

Cross-state voter comparison identifies double voters
CO and KS identify individuals who voted twice in 2010 election

Denver, Colorado - Secretary of State Scott Gessler today announced his office referred information to the FBI regarding individuals suspected of voting twice during the 2010 election. Following a comparison of voting records between Kansas and Colorado, six voters appear to have cast ballots in both states.

"Voter fraud undermines our electoral system," Secretary Gessler said. "I will continue to be vigilant and undertake these kinds of anti-fraud measures. These state crosschecks are an important component in ensuring the integrity of our election process."

Since 2009, Colorado has shared voter records with a consortium of states to monitor and identify cross-state voters. In 2008, four individuals were indicted by an Arizona grand jury for voting in both Colorado and Arizona. Now, following the 2010 election, the investigation has resulted in six cases of individuals who voted both in Colorado and Kansas.

The Colorado Secretary of State's office turned over information to the FBI that matched individual voter records including date of birth and signature on ballots cast in both Colorado and Kansas during the November 2010 election. In all six cases, the individuals voted either early or by mail ballot in Colorado; in five cases, the individual voted by mail ballot in Colorado and in one case, the individual voted during early voting in Colorado.

Persons convicted of voter fraud in Colorado can be sentenced to three years in prison and fines in excess of $1,000.

###

18-F-1517//0801
JA000197

USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 202 of 265

What does it cost to participate?

$0

18-F-1517//0802

JA000198

Kris W. Kobach

How Can a State Join the Crosscheck?

1. Chief State Election Official signs the Memorandum of Understanding (MOU)

2. CSEO assigns two staff members:
- one election administration person
- one IT person

3. Staff members will:
- participate in annual conference call and email
- pull VR data in January
- receive cross check results and process
- instruct local elections officials (respond to requests for addresses, signatures on poll books, etc.)

USCA Case #17-5171 Document #1680086 Filed: 08/18/2017 Page 203 of 285
18-F-1517//0803
JA000199

USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 204 of 265

18-F-1517//0804

Contact

Brad Bryant
State Election Director
Kansas Secretary of State's Office
brad.bryant@sos.ks.gov
785-296-4561

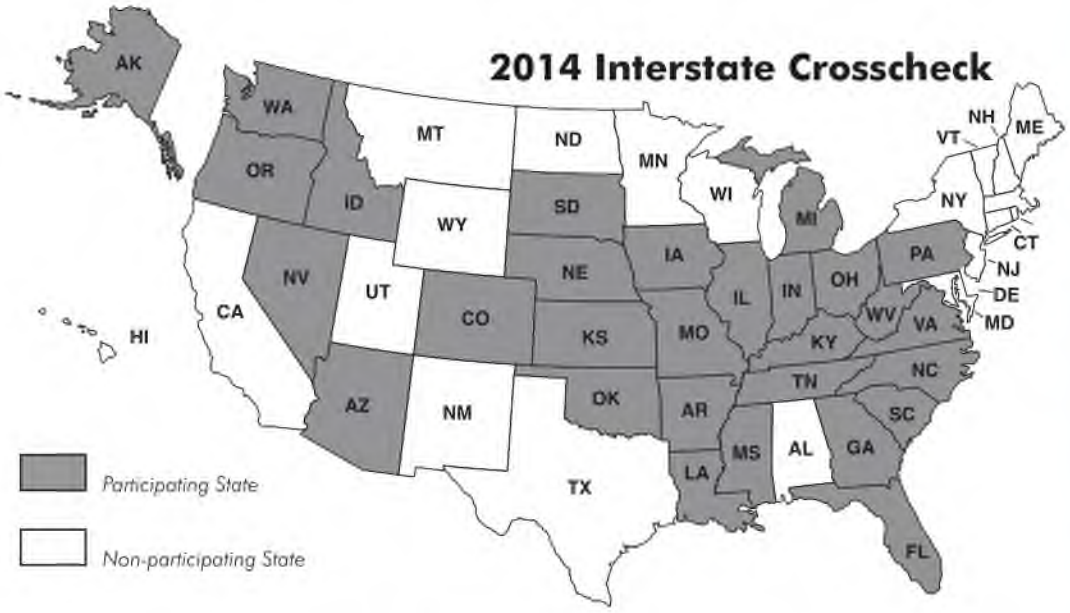
JA000200

canvassing kansas
AN UPDATE ON ELECTION NEWS FROM THE KANSAS SECRETARY OF STATE'S OFFICE

DECEMBER
2013

Interstate Crosscheck Program Grows

The ninth annual data comparison for the interstate voter registration crosscheck program will be run in January 2014. The program has grown from its original four midwest states (Iowa, Kansas, Missouri and Nebraska) to 29 states in 2014. In 2012 there were 15 participating states and in 2013 there were 22.



The interstate crosscheck program, administered by the Kansas Secretary of State's office, began in December 2005 when the secretaries representing the four original states signed a Memorandum of Understanding to coordinate their offices' efforts in several areas of election administration. Crosschecking voter registration data was one of the areas cited. The first crosscheck was conducted the next year, in 2006.

The program serves two purposes: (1) it identifies possible duplicate registrations among states, and (2) it provides evidence of possible double votes. Most states, including Kansas, process the duplicate registrations by mailing the individuals confirmation notices (as provided in the National Voter Registration Act of 1993) and placing the individuals' names in inactive status. Inactive voters are those for whom election officers have received evidence that they have moved out of the county or state. Once they are given inactive status, their registrations may be canceled if they fail to vote or otherwise contact the election office from the date of the confirmation notice through the second succeeding federal general (November) election.

Cont'd on pg. 6

IN THIS ISSUE

canvassing kansas

Published by the Office of the Secretary of State

EDITORS
Brad Bryant
Kay Curtis

LAYOUT AND DESIGN
Todd Caywood

CONTRIBUTORS
Brad Bryant
Kay Curtis

Suggestions or comments? Please call (785) 368-8095.

This publication may be duplicated for informational purposes only. No written permission is required with the exception of articles or information attributed to a source other than the Kansas Secretary of State.

© 2013

Kansas Secretary of State
Memorial Hall
120 SW 10th Ave.
Topeka, KS 66612-1594
(785) 296-4564

From the desk of the Secretary

"Lead, follow, or get out of the way."
Thomas Paine, 1737 - 1809. Kansas has consistently chosen the former when it comes to elections.

In 2005 Kansas took the lead when four states agreed to compare voter registration records with each other annually in order to identify duplicate voter registrations and double votes. Our IT department pulls data from a secure FTP site, runs comparisons and uploads the results to the FTP site on January 15 each year. Then each participating state can download its results and process them according to their own laws and regulations. The Interstate Voter Registration Crosscheck Program had increased to 14 participating states when I took office in 2011.

Convinced of the value of the program, I decided that I would make it one of my highest priorities to increase the number of participating states, hopefully doubling its size. The more states that participate, the more duplicate records each participating state can find. I contacted chief election officers in other states to explain how Crosscheck works and the value of this tool to maintain clean, current, and accurate voter lists to fight voter fraud. As a result, the number of states participating has more than doubled to 29 states that will share voter registration data in January 2014. While I am very pleased that over half of the 50 states are currently on board, I will continue to promote Crosscheck as an effective means of list maintenance.

In 2008 Kansas took the lead in helping voters to find election information when they need it by using internet search engines. As part of the Voting Information Project (VIP), Kansas contracted with ES&S to make programming changes to our ELVIS database so that all states with ES&S can provide a data feed to the VIP program which hosts the data. Google acknowledged our contribution by presenting a Kansas-shaped VIP award to the State of Kansas at the summer NASS conference.

Finally, in 2011 Kansas took the lead as the first state to combine three election-security policies: (1) requiring a government-issued photo ID for voting in person, (2) requiring either a Kansas driver's license number or photocopy of a current photo ID for applying for a mail-in ballot, and (3) requiring a document proving U.S. citizenship when a person registers to vote for the first time. Consequently, Kansas elections are the most secure in the nation against fraud.

Thank you for all you have done to help implement these reforms. Together we have made Kansas the nation's leader.

Kris W. Kobach

Voting Information Project Award Received at NASS

On July 19th, 2013, Google presented an award to recognize Kansas' efforts to improve the efficiency and effectiveness of elections through open data. Eight other states also received the award at the National Association of Secretaries of State 2013 Summer Conference in Anchorage, Alaska. Each of the nine states had participated in the Voting Information Project (VIP) by publishing polling places and other election data as part of the open data effort. Secretary of State Kris Kobach was present to accept the award for his office.

By joining the project on the ground floor, Kansas was among the first states to help registered voters to more readily find election information when they need it and where they are most likely to look for it. Government websites often are not the first place voters look. VIP is similar to the online VoterView feature of the Kansas voter registration system, and voters who perform Google searches for voter registration information will end up at the VoterView website as a result of the VIP.

In the run up to the 2012 general election, 22 million times users queried the Google Civic Information API. According to the VIP program, "When the project started in 2008, nobody involved knew whether the open data effort would have any impact at all. Early adopters took a risk on something new by agreeing to participate and the payoff was immense."

Google award presented to the state of Kansas for its contribution to the Voting Information Project.
Photo by Todd Caywood

The VIP program was initiated as a cooperative effort between the Pew Foundation and Google. As a private charitable organization, Pew's rules do not allow them to pay money to a private for-profit corporation, so Pew asked the Kansas SOS office to serve as a go-between. The SOS office wrote specifications and requested Election Systems & Software to make the required programming changes in the voter registration database. The cost of the programming was paid by Pew to the SOS office and passed on to ES&S. As a result, all states with ES&S databases benefit from the new functionality.

For more information about Kansas participation in the VIP project since 2008, see Canvassing Kansas, September 2010, page 6. ■

Clemens Receives CERA Certification

Crystal Clemens, Seward County Deputy Clerk/Election Officer, completed the Election Center's CERA program this year. Certificates were presented at the Election Center's annual national conference in Savannah, GA, held August 13-17, 2013. Crystal was one of fifty eight election officials to receive the award this year.

CERA (Certified Elections/Registration Administrator) is one of very few nationally recognized programs providing professional training for election administrators. The Election Center itself is a nationwide professional association of local, county and state voter registrars and election administrators that promotes training and best practices, monitors and lobbies on federal legislation, and provides a forum for the exchange of ideas.

Completion of the CERA program requires travel and attendance at a number of training sessions across the country over a period of years. Crystal is one of a small handful of Kansas election officials who have completed it.

Crystal's supervisor, Seward County Clerk Stacia Long, had this to say: "Crystal has always shown great passion for the entire election process. I am very proud of her designation as a CERA. She truly is a great asset to the Election Office and Seward County." ■

Attorney General Issues Opinion on Concealed Carry

The office of Attorney General Derek Schmidt issued a formal opinion on November 27, 2013 in response to questions posed by Secretary of State Kris Kobach. Kobach requested the opinion in a letter dated September 30, 2013, as chief state election officer and on behalf of county election officers across the state.

The issue at the heart of the request was how polling places would be affected by passage of the Personal and Family Protection Act of 2013. The Act, passed as Senate Substitute for House Bill 2052 (2013 Kansas Session Laws, Chapter 105), authorizes persons who possess concealed carry permits to carry weapons into municipal buildings except under specific circumstances. "Municipal building" includes any facility owned or leased by a municipality, which could include facilities used as polling places during advance voting or on election day.

In his letter, Secretary Kobach asked the following questions:

1. ***Does the Act apply to privately-owned facilities used as polling places by verbal agreement?***

2. ***Does the Act apply to privately-owned facilities used as polling places by written agreement when no rent money is paid to the owner or manager of the site?***

3. ***Does the Act apply to privately-owned facilities used as polling places by written agreement when rent money is paid to the owner or manager of the site?***

4. ***If only one room or one portion of a building otherwise not subject to the Act is used as a polling place, does the Act apply to the entire building or only to the area used as a polling place?***

5. ***If an area in a nursing home, assisted living center or long term care facility is used for mobile advance voting pursuant to K.S.A. 25-2812, does the Act apply to the voting area?***

6. ***Do the provisions of the Act applicable to schools still apply to school facilities used as polling places?***

7. ***Is a county government liable for claims of denial of equal protection if various polling places have different levels of security as a result of implementation of the Act?***

At the time of this writing, the secretary of state had just begun to analyze the opinion. The SOS office will communicate further information to CEOs when the analysis is complete. In the meantime, CEOs are encouraged to discuss the opinion with their county attorneys and counselors. The full opinion may be found online: ***http://ksag.washburnlaw.edu/opinions/2013/2013-020.pdf***.

The synopsis from Attorney General Opinion 2013-20 is reproduced here:

Except as described herein, the use of real property as a polling place does not transform the nature of that property for the purposes of the PFPA. Any concealed carry requirements that applied to that property immediately before its temporary use as a polling place continue to apply during its use as a polling place and thereafter.

The Personal and Family Protection Act (PFPA) authorizes concealed carry licensees to carry a concealed handgun into a polling place to the extent that concealed handguns are permitted to be carried into the building in which the polling place is located.

The provisions of K.S.A. 2013 Supp. 75-7c20 apply only to buildings that are owned or leased in their entirety by the state or a municipality. If the PFPA requires concealed carry to be permitted in a state or municipal building, then concealed carry licensees must be permitted to carry a concealed handgun in all parts of the building, including areas used as polling places, with the exception of courtrooms, ancillary courtrooms, and secure areas of correctional facilities, jails and law enforcement agencies.

The governing body or chief administrative officer, if no governing body exists, of a state or municipal building may exempt the building from the provisions of K.S.A. 2013 Supp. 75-7c20 for a set period of time. If a state or municipal building is so exempted, concealed carry may be prohibited by posting the building in accordance with K.S.A. 2013 Supp. 75-7c10.

Cont'd on pg. 6

SOS Office Involved in Litigation

The office of the Kansas Secretary of State finds itself involved in three lawsuits that could affect the voter registration process and the 2014 elections. All are related to the 2011 Kansas SAFE Act. One case deals with the photo ID requirement and the other two deal with the requirement that new voters prove their U.S. citizenship the first time they register to vote.

1. Arthur Sprye and Charles Hamner v. Kris W. Kobach
In a suit filed November 1, 2013, two Osage County voters challenged the constitutionality of the photo ID requirement.

2. Kris W. Kobach, Kansas Secretary of State; and Ken Bennett, Arizona Secretary of State; v. United States Election Assistance Commission
In a suit filed in U.S. District Court in Kansas on August 21, 2013, the Kansas and Arizona Secretaries of State asked for a ruling to require the Election Assistance Commission to include the citizenship requirement in the voter instructions accompanying the universal federal voter registration application form, which is prescribed by the EAC. This lawsuit is in response to the June 17, 2013 ruling by the U.S. Supreme Court in Arizona v. Inter Tribal Council of Arizona regarding the constitutionality of states' requirements that voters provide proof of citizenship. The Court's ruling indicated that states might file suit if the EAC declined to make the necessary changes to the voter registration form administratively.

3. Aaron Belenky, Scott Jones, and Equality Kansas v. Kris Kobach, Kansas Secretary of State, and Brad Bryant, Kansas Elections Director
In a suit filed November 21, 2013, the plaintiffs seek declaratory and injunctive relief to keep the secretary of state's office from implementing a dual voter registration system. The SOS office had developed contingency plans to administer voter registration and ballots to individuals who attempted to register using the universal federal form but who had not provided proof of U.S. citizenship in compliance with Kansas law. No actions have been taken to implement the plan, and no federal elections have occurred in which federal-only ballots were administered to these voters. (See also Canvassing Kansas, September 2013, page 1.)

The goal of the secretary of state's office is to have the cases decided as soon as possible so CEOs and poll workers will know the rules before preparations begin for the 2014 election season. ■

Kobach Reappoints Lehman

Secretary of State Kris Kobach reappointed Tabitha Lehman as Sedgwick County Election Commissioner in September 2013. Her regular term expires on July 19, 2017. This will be Lehman's first full term as election commissioner, having been appointed to fill an unexpired term in 2011.

Lehman was appointed in November 2011 to succeed Bill Gale who resigned his position to pursue other employment. Gale had been appointed in November 2003 to succeed Marilyn Chapman, and he was reappointed in July 2009.

Speaking of her reappointment, Lehman said:
"I appreciate the opportunity to continue serving the voters of Sedgwick County and look forward to providing them with safe and efficient elections in the coming four years." ■


Sedgwick County Election Commissioner Tabitha Lehman
Photo courtesy of Tabitha Lehman

Crosscheck
Cont'd

Evidence of double votes is presented to law enforcement officers for investigation and possible prosecution. The referral is usually made to county law enforcement officers, but state or federal officials may be involved in some cases.

States join the crosscheck by signing a Memorandum of Understanding. The chief state election officer (usually the secretary of state) or a designee may sign the MOU for a given state.

Participating states pull their entire voter registration databases and upload them to a secure FTP site on January 15 each year. The Kansas SOS office IT staff pull the states' data from the FTP site, run the comparison, and upload each state's results to the FTP site. Each state then pulls its results from the FTP site and processes them according to its individual laws, regulations and procedures. In Kansas, results are provided to CEOs with instructions for analyzing them and mailing confirmation notices.

The crosscheck program is one of several list maintenance programs used to keep registration records up to date. (See also Canvassing Kansas, March 2010, page 9.) ■

Attorney General
Cont'd

If the governing body or chief administrative officer of a state or municipal building does not exempt a building from the provisions of K.S.A. 2013 Supp. 75-7c20, then concealed carry licensees must be permitted to carry a concealed handgun inside the building unless adequate security measures are provided and the building is posted as prohibiting concealed carry.

Concealed carry is not required to be permitted in a polling place located inside a privately-owned building unless the county has leased the entire privately-owned building.

Concealed carry is not required to be permitted in polling places located inside public school district buildings because a public school district is not a municipality for the purposes of the PFPA.

An equal protection claim against a county based upon the varying ability of concealed carry licensees to carry a concealed handgun into a polling place would be subject to the rational basis test. ■

Jury List Program Initiated

A 2013 law which went into effect July 1, 2013, requires district courts in Kansas to provide to the secretary of state the names of prospective jurors who indicate on their jury questionnaires that they are not United States citizens. Noncitizens are exempt from jury duty. The secretary of state passes the names on to CEOs for review. If they are found to be registered voters, their registrations are canceled. (See 2013 House Bill 2164; 2013 Kansas Session Laws Chapter 85.)

The relevant section of the law is New Section 1, reproduced below. Most of the bill deals with grand juries.

New Section 1. (a) On and after July 1, 2013, any jury commissioner that receives information regarding citizenship from a prospective juror or court of this state that disqualifies or potentially disqualifies such prospective juror from jury service pursuant to K.S.A. 43-156, and amendments thereto, shall submit such information to the secretary of state in a form and manner approved by the secretary of state. Any such information provided by a jury commissioner to the secretary of state shall be limited to the information regarding citizenship and the full name, current and prior addresses, age and telephone number of the prospective juror, and, if available, the date of birth of the prospective juror. Any such information provided by a jury commissioner to the secretary of state shall be used for the purpose of maintaining voter registrations as required by law.

The secretary of state's office worked with the Office of Judicial Administration (OJA) to design the following procedure to comply with the law:

- The clerk in each of Kansas' 31 judicial districts will submit a monthly report directly to the SOS office containing names of persons who were exempted from jury duty on the basis of their claims to be non-U.S. citizens.
- Reports will be submitted via email on or after the 15th of each month beginning in December 2013.
- The SOS will notify OJA of missing reports. OJA will contact any such district court clerks to remind them to submit their reports.
- If any of the persons listed in the reports are found to be registered voters and their citizenship status is not in doubt, their names will be sent by the SOS office to the appropriate county election officers with instructions regarding the possible cancellation of the persons' voter registration records. ■

State Fair Opinion Poll Results

The Office of the Secretary of State has operated a booth in the Meadowlark Building at the Kansas State Fair in Hutchinson for more than 25 years. The dates of the fair this year were September 6-15. This was the 100th anniversary of the fair, and the theme was "Never Gets Old."

At the booth, the SOS office provides information about agency activities, registers voters, and conducts an opinion poll on current issues. Don Merriman, Saline County Clerk, has assisted the SOS office for many years by lending ES&S iVotronic voting machines to help the fair visitors familiarize themselves with electronic voting technology. We want to recognize and thank Don for his assistance and the Lockwood Company for its donation of ballot programming services.

The SOS booth is mostly staffed by agency employees, but sometimes county election office personnel help out by volunteering to work in the booth. This year's county volunteers were: Sharon Seibel, Ford County Clerk; Debbie Cox, Ford County Deputy Clerk; Donna Maskus, Ellis County Clerk; Don Merriman, Saline County Clerk; Crysta Torson, Lane County Clerk; and Karen Duncan, Lane County Deputy Clerk. Thanks to the volunteers for helping out!

Following are the results of the opinion poll:

Question #1: New Kansas voters must provide proof of citizenship when registering to vote.

709 *I approve of this requirement.*
96 *I do not approve of this requirement.*
27 *I have no opinion about this requirement.*

Question #2: Which university will advance the furthest in the 2014 NCAA Men's Basketball Tournament?

397 *University of Kansas*
196 *Kansas State University*
179 *Wichita State University*
48 *None will make the tournament*

Question #3: Which of these alleged abuses of power by the federal government is the most concerning to you?

342 *NSA secretly collecting phone records of millions of U.S. citizens.*
332 *IRS intentionally discriminating against conservative organizations.*
153 *Presidential political appointees using secret email accounts to conduct official government business.*
132 *White House's sweeping seizure of Associated Press records and cable television documents.*

Question #4: Should the Internal Revenue Service be abolished?

526 *Yes. A flat or fair tax is simpler, cheaper and easier to manage.*
86 *Yes. We shouldn't have to pay income tax anyway.*
125 *No. Better training and oversight will fix most problems.*
2 *No. There is nothing wrong with the IRS.*

Question #5: Who is your favorite super hero?

90 *Xena: Warrior Princess*
379 *Superman*
94 *Wonder Woman*
195 *Batman* ■

Former Longtime Neosho County Clerk Dies

Wayne B. Gibson, Jr., a well known longtime county clerk from Neosho County, died on September 18, 2013, at a hospital in Labette County. Wayne served many years in the Neosho County Clerk's office and was known to Kansas election officials as a hardworking, conscientious public servant.

Gibson started working in the county clerk's office on January 16, 1961 and became Deputy Clerk about a month later. He then became Clerk on July 14, 1971, following the death of his predecessor, Virgil Lowe. Gibson served continuously until his retirement on April 20, 2007. During that time he was elected ten times - in 1972, 1974, 1976, 1980, 1984, 1988, 1992, 1996, 2000 and 2004.

The vacancy created by Gibson's resignation was filled by Randal Neely, who took office on August 1, 2007, and continues in office today. ■

Dominion Seeks Voting System Certification

Dominion Voting Systems, Inc., submitted a letter dated October 4, 2013 requesting certification of its Democracy Suite Version 4.14 voting system. According to Kansas law, a manufacturer seeking certification of its voting system must submit a formal letter, pay a $500 fee, and demonstrate the system at a certification hearing held in Topeka.

A hearing was held at the secretary of state's office on November 21, 2013, attended by Secretary of State Kris Kobach and members of his staff. The Democracy Suite system was demonstrated and explained by Norma Townsend, Don Vopalensky, Jeff Hintz and Michael Kelava. Dominion is represented in Kansas by its subcontractor, Election Source. Dominion also markets and services Premier (formerly Diebold) voting equipment, having purchased Premier from Election Systems and Software several years ago. ES&S still sells and services Premier equipment along with its own system, but Dominion owns the intellectual property rights of Premier equipment as a result of its purchase of the company.

As of this writing, Secretary Kobach has not certified the Dominion Democracy Suite. CEOs will be notified if and when certification is granted.

The Democracy Suite is a paper optical scan-based system which includes precinct ballot scanners and central scanners. The accessible ADA- and HAVA-compliant device allows a voter with a visual impairment to record his/her choices using an audio ballot and keypad. The system prints an optical scan ballot that is scanned along with other ballots. ■

Sedgwick County Sued Over Ballot Records

Sedgwick County Election Commissioner Tabitha Lehman was sued by a person seeking public access to Real Time Audit Logs (RTALs) on electronic voting machines. RTAL is ES&S's trade name for a voter verifiable paper audit trail (VVPAT), which is a printable electronic record of each voter's actions on the voting machine. RTAL documents are viewable by the voter before the electronic ballot is cast. Once the voter has cast the ballot the documents are randomly stored in the system's memory.

Elizabeth Clarkson v. Sedgwick County Elections Commissioner Tabitha Lehman was filed in state district court in Sedgwick County on June 18, 2013. The plaintiff sought access to RTAL records pursuant to the Kansas Open Records Act in order to conduct a post-election audit of the results of the November 2010 election.

In response to the plaintiff's original request for records, the election office provided precinct-based results tapes but denied the request for individual ballot logs, citing K.S.A. 25-2422 and the unnecessary burden and expense required to produce the records. State law does provide limited access to election records in a recount, but the law does not have specific provisions related to VVPATs or RTALs. These arguments were detailed in a response filed in court in July.

The court ruled in favor of the election commissioner's office. ■

SOS Holiday Hours

In observance of the regular calendar of state holidays, the secretary of state's office will be closed on the following dates:

December 25, 2013, for Christmas Day, and **January 1, 2014,** for New Year's Day.

In addition, the office will be closed Monday, **January 20, 2014** in observance of Martin Luther King, Jr. Day.

Happy Holidays from the SOS office!

PRIVACY IMPACT ASSESSMENT (PIA)

For the

SAFE - SAFE ACCESS FILE EXCHANGE

Aviation and Missile Research, Development, and Engineering Center; RDECOM

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: DA305750
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☐ **Yes**
- ☒ **No**

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The U.S. Army Aviation and Missile Research Development and Engineering Center (AMRDEC) Safe Access File Exchange system is designed for securely exchanging various types of electronic files. It was created to provide users the capability to send/receive large files. Safe Access File Exchange primary function is strictly used as a transfer mechanism for large data files. Safe Access File Exchange can be used by anyone sending files to individuals with a .mil or .gov e-mail addresses. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format. SAFE use the latest web browser transport encryption protocols.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The security risk associated with maintaining PII in an electronic environment has been identified and mitigated through administrative, technical, and physical safeguards as well as with policy and procedures for handling, using, maintaining PII and training for authorized users of PII data. Due to the stringent safeguards and access requirements, the system and data are secure and it is unlikely that the data would be compromised or provided to any unauthorized individuals or agencies.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

☒ **Other DoD Components.**

Specify. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

☒ **Other Federal Agencies.**

Specify. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

☒ **State and Local Agencies.**

Specify. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

By not Sending any PII through the SAFE transfer system.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

By not Sending any PII through the SAFE transfer system.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- ☐ **Privacy Act Statement**
- ☐ **Privacy Advisory**
- ☐ **Other**
- ☒ **None**

Describe each applicable format.

Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

Administration of Barack Obama, 2015

Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology

March 19, 2015

Memorandum for the Secretary of Defense, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the National Security Advisor, and the Director of the Office of Administration

Subject: Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to improve the information resources and information systems provided to the President, Vice President, and Executive Office of the President (EOP), I hereby direct the following:

Section 1. Policy. The purposes of this memorandum are to ensure that the information resources and information systems provided to the President, Vice President, and EOP are efficient, secure, and resilient; establish a model for Government information technology management efforts; reduce operating costs through the elimination of duplication and overlapping services; and accomplish the goal of converging disparate information resources and information systems for the EOP.

This memorandum is intended to maintain the President's exclusive control of the information resources and information systems provided to the President, Vice President, and EOP. High-quality, efficient, interoperable, and safe information systems and information resources are required in order for the President to discharge the duties of his office with the support of those who advise and assist him, and with the additional assistance of all EOP components. The responsibilities that this memorandum vests in the Director of White House Information Technology, as described below, have been performed historically within the EOP, and it is the intent of this memorandum to continue this practice.

The Director of White House Information Technology, on behalf of the President, shall have the primary authority to establish and coordinate the necessary policies and procedures for operating and maintaining the information resources and information systems provided to the President, Vice President, and EOP. Nothing in this memorandum may be construed to delegate the ownership, or any rights associated with ownership, of any information resources or information systems, nor of any record, to any entity outside of the EOP.

Sec. 2. Director of White House Information Technology. (a) There is hereby established the Director of White House Information Technology (Director). The Director shall be the senior officer responsible for the information resources and information systems provided to the President, Vice President, and EOP by the Presidential Information Technology Community (Community). The Director shall:

(i) be designated by the President;

(ii) have the rank and status of a commissioned officer in the White House Office; and

(iii) have sufficient seniority, education, training, and expertise to provide the necessary advice, coordination, and guidance to the Community.

(b) The Deputy Chief of Staff for Operations shall provide the Director with necessary direction and supervision.

(c) The Director shall ensure the effective use of information resources and information systems provided to the President, Vice President, and EOP in order to improve mission performance, and shall have the appropriate authority to promulgate all necessary procedures and rules governing these resources and systems. The Director shall provide policy coordination and guidance for, and periodically review, all activities relating to the information resources and information systems provided to the President, Vice President, and EOP by the Community, including expenditures for, and procurement of, information resources and information systems by the Community. Such activities shall be subject to the Director's coordination, guidance, and review in order to ensure consistency with the Director's strategy and to strengthen the quality of the Community's decisions through integrated analysis, planning, budgeting, and evaluation processes.

(d) The Director may advise and confer with appropriate executive departments and agencies, individuals, and other entities as necessary to perform the Director's duties under this memorandum.

Sec. 3. Executive Committee for Presidential Information Technology. There is hereby established an Executive Committee for Presidential Information Technology (Committee). The Committee consists of the following officials or their designees: the Assistant to the President for Management and Administration; the Executive Secretary of the National Security Council; the Director of the Office of Administration; the Director of the United States Secret Service; and the Director of the White House Military Office.

Sec. 4. Administration. (a) The President or the Deputy Chief of Staff for Operations may assign the Director and the Committee any additional functions necessary to advance the mission set forth in this memorandum.

(b) The Committee shall advise and make policy recommendations to the Deputy Chief of Staff for Operations and the Director with respect to operational and procurement decisions necessary to achieve secure, seamless, reliable, and integrated information resources and information systems for the President, Vice President, and EOP. The Director shall update the Committee on both strategy and execution, as requested, including collaboration efforts with the Federal Chief Information Officer, with other government agencies, and by participating in the Chief Information Officers Council.

(c) The Secretary of Defense shall designate or appoint a White House Technology Liaison for the White House Communications Agency and the Secretary of Homeland Security shall designate or appoint a White House Technology Liaison for the United States Secret Service. Any entity that becomes a part of the Community after the issuance of this memorandum shall designate or appoint a White House Technology Liaison for that entity. The designation or appointment of a White House Technology Liaison is subject to the review of, and shall be made in consultation with, the President or his designee. The Chief Information Officer of the Office of Administration and the Chief Information Officer of the National Security Council, and their successors in function, are designated as White House Technology Liaisons for their respective components. In coordination with the Director, the White House Technology Liaisons shall ensure that the day-to-day operation of and long-term

strategy for information resources and information systems provided to the President, Vice President, and EOP are interoperable and effectively function as a single, modern, and high-quality enterprise that reduces duplication, inefficiency, and waste.

(d) The President or his designee shall retain the authority to specify the application of operating policies and procedures, including security measures, which are used in the construction, operation, and maintenance of any information resources or information system provided to the President, Vice President, and EOP.

(e) Presidential Information Technology Community entities shall:

(i) assist and provide information to the Deputy Chief of Staff for Operations and the Director, consistent with applicable law, as may be necessary to implement this memorandum; and

(ii) as soon as practicable after the issuance of this memorandum, enter into any memoranda of understanding as necessary to give effect to the provisions of this memorandum.

(f) As soon as practicable after the issuance of this memorandum, EOP components shall take all necessary steps, either individually or collectively, to ensure the proper creation, storage, and transmission of EOP information on any information systems and information resources provided to the President, Vice President, and EOP.

Sec. 5. Definitions. As used in this memorandum:

(a) "Information resources," "information systems," and "information technology" have the meanings assigned by section 3502 of title 44, United States Code.

(b) "Presidential Information Technology Community" means the entities that provide information resources and information systems to the President, Vice President, and EOP, including:

(i) the National Security Council;

(ii) the Office of Administration;

(iii) the United States Secret Service;

(iv) the White House Military Office; and

(v) the White House Communications Agency.

(c) "Executive Office of the President" means:

(i) each component of the EOP as is or may hereafter be established;

(ii) any successor in function to an EOP component that has been abolished and of which the function is retained in the EOP; and

(iii) the President's Commission on White House Fellowships, the President's Intelligence Advisory Board, the Residence of the Vice President, and such other entities as the President from time to time may determine.

Sec. 6. General Provisions. (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, entity, office, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

Categories: Communications to Federal Agencies : White House Information Technology, Director, memorandum establishing; Executive Committee for Presidential Information Technology, memorandum establishing.

Subjects: White House Office : Assistants to the President :: White House Information Technology, Director; White House Office : Information Technology, Executive Committee for Presidential.

DCPD Number: DCPD201500185.

USCA Case #17-5171 Document #1689466 Filed: 08/18/2017 Page 223 of 265

the WHITE HOUSE

From the Press Office

Speeches & Remarks

Press Briefings

Statements & Releases

Nominations & Appointments

Presidential Actions

Legislation

Disclosures

The White House
Office of the Vice President

For Immediate Release June 28, 2017

Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity

This morning, Vice President Mike Pence held an organizational call with members of the Presidential Advisory Commission on Election Integrity. The Vice President reiterated President Trump's charge to the commission with producing a set of recommendations to increase the American people's confidence in the integrity of our election systems.

"The integrity of the vote is a foundation of our democracy; this bipartisan commission will review ways to strengthen that integrity in order to protect and preserve the principle of one person, one vote," the Vice President told commission members today.

The commission set July 19 as its first meeting, which will take place in Washington, D.C.

USCA Case #17-5171 Document #1689466 Filed: 09/18/2017 Page 224 of 265

Vice Chair of the Commission and Kansas Secretary of State Kris Kobach told members a letter will be sent today to the 50 states and District of Columbia on behalf of the Commission requesting publicly-available data from state voter rolls and feedback on how to improve election integrity.

Presidential Advisory Commission on Election Integrity

June 28, 2017

The Honorable Elaine Marshall
Secretary of State
PO Box 29622
Raleigh, NC 27626-0622

Dear Secretary Marshall,

I serve as the Vice Chair for the Presidential Advisory Commission on Election Integrity ("Commission"), which was formed pursuant to Executive Order 13799 of May 11, 2017. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President of the United States that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine the American people's confidence in the integrity of federal elections processes.

As the Commission begins it work, I invite you to contribute your views and recommendations throughout this process. In particular:

1. What changes, if any, to federal election laws would you recommend to enhance the integrity of federal elections?
2. How can the Commission support state and local election administrators with regard to information technology security and vulnerabilities?
3. What laws, policies, or other issues hinder your ability to ensure the integrity of elections you administer?
4. What evidence or information do you have regarding instances of voter fraud or registration fraud in your state?
5. What convictions for election-related crimes have occurred in your state since the November 2000 federal election?
6. What recommendations do you have for preventing voter intimidation or disenfranchisement?
7. What other issues do you believe the Commission should consider?

In addition, in order for the Commission to fully analyze vulnerabilities and issues related to voter registration and voting, I am requesting that you provide to the Commission the publicly-available voter roll data for North Carolina, including, if publicly available under the laws of your state, the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social

security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.

You may submit your responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE"), which is a secure FTP site the federal government uses for transferring large data files. You can access the SAFE site at https://safe.amrdec.army.mil/safe/Welcome.aspx. We would appreciate a response by July 14, 2017. Please be aware that any documents that are submitted to the full Commission will also be made available to the public. If you have any questions, please contact Commission staff at the same email address.

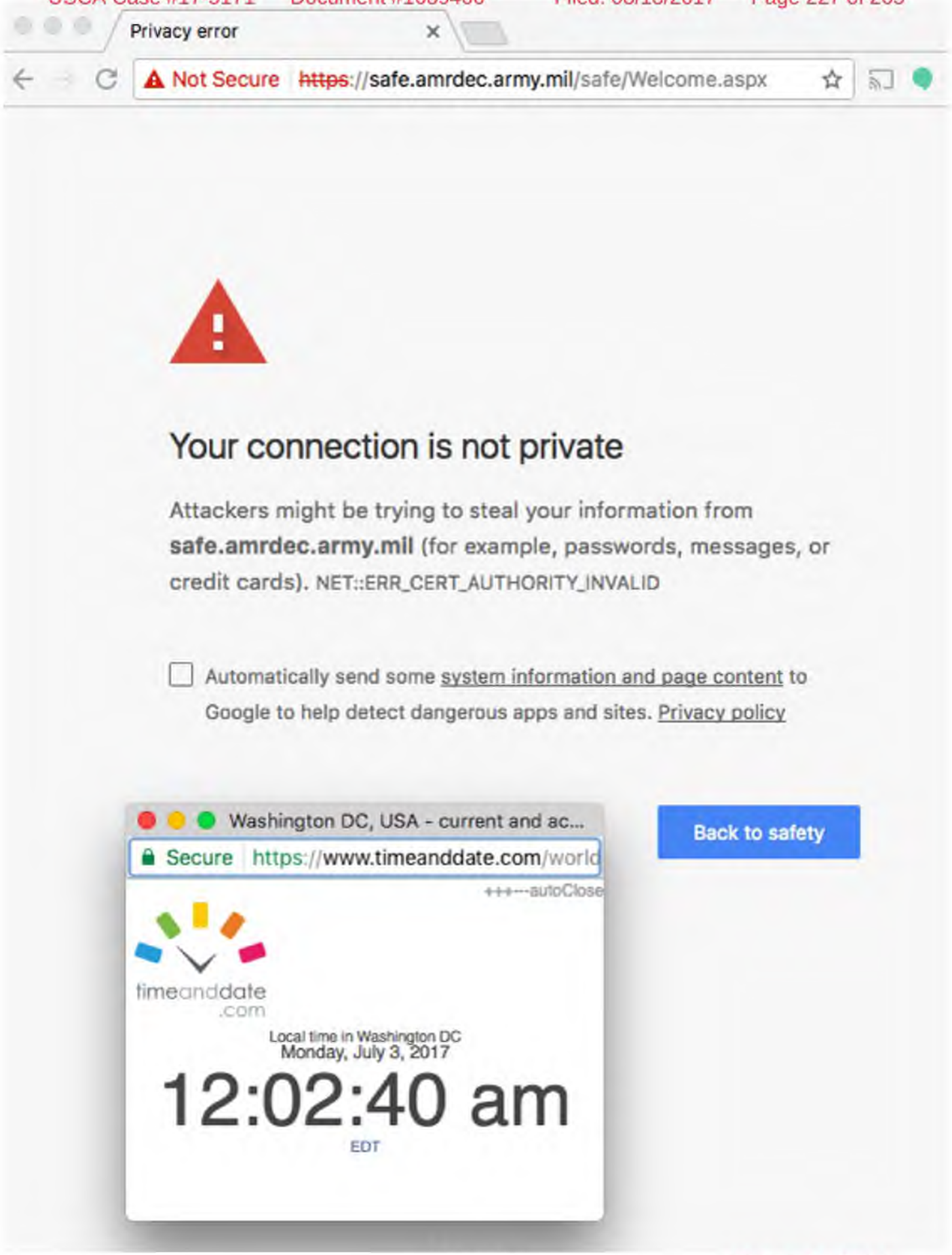
On behalf of my fellow commissioners, I also want to acknowledge your important leadership role in administering the elections within your state and the importance of state-level authority in our federalist system. It is crucial for the Commission to consider your input as it collects data and identifies areas of opportunity to increase the integrity of our election systems.

I look forward to hearing from you and working with you in the months ahead.

Sincerely,

Kris Kobach

Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity


Privacy error
Not Secure https://safe.amrdec.army.mil/safe/Welcome.aspx
Your connection is not private
Attackers might be trying to steal your information from safe.amrdec.army.mil (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID
Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy
Back to safety
Washington DC, USA - current and ac...
Secure https://www.timeanddate.com/world
timeanddate.com
Local time in Washington DC
Monday, July 3, 2017
12:02:40 am
EDT

July 3, 2017

National Association of State Secretaries
444 North Capitol Street NW, Suite 401
Washington, DC 20001

Dear State Secretaries:

We write to you regarding the recent letter from the Presidential Advisory Commission on Election Integrity ("PACEI") to state election officials, requesting detailed personal information from your state voter registration records.[1] We are technical experts, legal scholars, and representatives of organizations expert in election integrity, voting verification, and voter privacy. We strongly oppose the PACEI request for voter record information and urge you not to comply.

The PACEI is seeking:

> "the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information."

This is sensitive, personal information that individuals are often required to provide to be eligible to vote. There is no indication how the information will be used, who will have access to it, or what safeguards will be established.[2] Moreover, it appears that the Presidential Commission has failed to undertake and publish a Privacy Impact Assessment, required by federal law, prior to the collection of personal data.[3]

Although the standards vary across the country, there is no question that voter privacy -- and the secret ballot in particular – are integral to the American system of democracy. It is absolutely unprecedented for the federal government to demand the production of voter records from the states.

As custodians of voter data, you have a specific responsibility to safeguard voter record information. We urge you to protect the rights of the voters in your states and to oppose the request from the PACEI.

---

[1] *See, e.g.,* Letter from Kris W. Kobach, Vice Chair, PACEI, to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017).
[2] *See* EPIC, "Voter Privacy and the PACEI," epic.org/privacy/voter/pacei/.
[3] Pub.Law 107-347, 44 U.S.C. § 3501 (Note). *See also* "M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" (Sept. 26, 2003).

For further information regarding this statement, please contact EPIC President Marc Rotenberg (rotenberg@epic.org) or EPIC Policy Director Caitriona Fitzgerald (fitzgerald@epic.org).

ORGANIZATIONS

Electronic Privacy Information Center (EPIC)
American Library Association
Center for Democracy & Technology
Center for Media and Democracy
Center for Media Justice
Constitutional Alliance
Consumer Federation of America
Consumer Action
Consumer Watchdog
Cyber Privacy Project
Defending Rights & Dissent
Federation of American Scientists
Government Accountability Project
Lawyers for Good Government
Liberty Coalition
National Center for Transgender Equality
National Network to End Domestic Violence
New America's Open Technology Institute
Patient Privacy Rights
Privacy Rights Clearinghouse
Privacy Times
RootsAction.org
World Privacy Forum

INDIVIDUAL EXPERTS

Alessandro Acquisti, Professor, Carnegie Mellon University
Ann Bartow, Professor of Law, University of New Hampshire School of Law
Francesca Bignami, Professor of Law, The George Washington University Law School
Christine L. Borgman, Distinguished Professor & Presidential Chair in Information Studies, UCLA
Kimberly Bryant, Founder/Executive Director, Black Girls CODE
David Chaum, Voting Systems Institute
Danielle Keats Citron, Morton & Sophia Macht Professor of Law, University of Maryland Carey School of Law
Julie E. Cohen, Mark Claster Mamolen Professor of Law and Technology, Georgetown Law
Jennifer Daskal, Associate Professor, American University Washington College of Law
Cynthia Dwork, Distinguished Scientist, Microsoft Research

David J. Farber, Distinguished Career Professor of Computer Science and Public Policy, Carnegie Mellon University
Michael Fischer, Professor of Computer Science, Yale University
Martin Hellman, Member, US National Academy Engineering, Professor Emeritus of Electrical Engineering, Stanford University
Candice Hoke, Co-Director, Center for Cybersecurity & Privacy Protection, Professor of Law, C|M Law, Cleveland State University
Deborah Hurley, Harvard University and Brown University
Dr. David Jefferson, Visiting Scientist, Lawrence Livermore National Laboratory
Jeff Jonas, Founder and Chief Scientist, Senzing
Douglas W. Jones, Department of Computer Science, University of Iowa, coauthor of *Broken Ballots: Will Your Vote Count*, CSLI, 2012
Lou Katz, Ph.D., founder, Usenix Association
Pamela S. Karlan, Kenneth and Hale Montgomery Professor of Public Interest Law, Co-Director, Supreme Court Litigation Clinic, Stanford Law School
Joe Kiniry, CEO and Chief Scientist, Free & Fair
Chris Larsen, Executive Chairman, Ripple, Inc.
Harry Lewis, Gordon McKay Professor of Computer Science, Harvard University
Anna Lysyanskaya, Professor of Computer Science, Brown University
Gary T. Marx, Professor Emeritus of Sociology, MIT
Mary Minow, Senior Fellow, Advanced Leadership Initiative, Harvard University
Dr. Pablo Molina, Adjunct Professor, Georgetown University
Jennifer L. Mnookin, Dean and David G. Price & Dallas P. Price Professor of Law, UCLA School of Law
Eben Moglen, Professor of Law, Columbia Law School
Erin Murphy, Professor of Law. NYU School of Law
Peter G. Neumann, Computer Science Laboratory, SRI International
Helen Nissenbaum, Professor, NYU + Cornell Tech
Frank Pasquale, Professor of Law, University of Maryland Carey School of Law
Ron Rivest, MIT Institute Professor
Pam Samuelson, Richard M. Sherman Distinguished Professor of Law, Berkeley Law School
Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School
Barbara Simons, Ph.D., IBM Research (retired)
Robert Ellis Smith, publisher, *Privacy Journal*
Eugene H. Spafford, Professor, Purdue University
Philip B. Stark, Associate Dean, Mathematical and Physical Sciences, Professor, Department of Statistics, University of California
Nadine Strossen, John Marshall Harlan II Professor of Law, New York Law School; Former President, American Civil Liberties Union
Frank Turkheimer, Professor of Law Emeritus, University of Wisconsin Law School
Sherry Turkle, Abby Rockefeller Mauzé Professor of the Social Studies of Science and Technology, Massachusetts Institute of Technology
Poorvi L. Vora, Professor of Computer Science, The George Washington University

Jim Waldo, Gordon McKay Professor of the Practice, Chief Technology Officer, Harvard University
Anne L. Washington, Assistant Professor, Schar School of Policy and Government, George Mason University
Chris Wolf, Board Chair, Future of Privacy Forum
Shoshana Zuboff, Charles Edward Wilson Professor of Business Administration, Retired

(affiliations are for identification only)

The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

2 Martin Luther King Jr., Drive
802 West Tower
Atlanta, Georgia 30334

Chris Harvey
DIRECTOR OF ELECTIONS

July 3, 2017

VIA EMAIL
The Honorable Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity
ElectionIntegrityStaff@ovp.eop.gov

RE: Open Records Request Dated June 28, 2017

Dear Secretary Kobach,

This letter is in response to your request dated June 28, 2017 in which you seek the publicly-available voter roll data for Georgia. Under Georgia law (O.C.G.A. § 21-2-225), information on file regarding Georgia's list of electors is required to be available to the public upon request, except that the day and month of birth, social security number, driver's license number, and the locations at which electors applied to vote are confidential and not subject to disclosure.

Two years ago, our office reformed its process of handling public record requests to be more secure. In order to provide the publicly available information, our security protocol requires certain steps to be followed. Upon receipt, our office will prepare the publicly-available list of electors data file. The data file will undergo a thorough review process to ensure confidential information is not included before it is sent by secure means to the Commission. The data file will be encrypted and password protected.

Also, in order to process and send the requested publicly-available records, our office requires pre-payment of the $250 statewide file fee. Please send check or money order payable to the "Georgia Secretary of State" to my attention at the address in the header of this letter.

Sincerely,

Chris Harvey
Director of Elections
Georgia Secretary of State's Office

DECLARATION OF MARC ROTENBERG

I, Marc Rotenberg, declare as follows:

1. I am President and Executive Director for the Plaintiff Electronic Privacy Information Center ("EPIC").

2. Plaintiff EPIC is a non-profit corporation located in Washington, D.C. EPIC is a public interest research center, which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has a particular interest in preserving privacy safeguards established by Congress, including the E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note), EPIC pursues a wide range of activities designed to protect privacy and educate the public, including policy research, public speaking, conferences, media appearances, publications, litigation, and comments for administrative and legislative bodies regarding the protection of privacy.

3. I am a member in good standing of the Bar of the District of Columbia (admitted 1990), the Bar of Massachusetts (1987), the U.S. Supreme Court (1991), the U.S. Court of Appeals—1st Circuit (2005), the U.S. Court of Appeals—2nd Circuit (2010), the U.S. Court of Appeals—3rd Circuit (1991) the U.S. Court of Appeals—4th Circuit (1992), the U.S. Court of Appeals—5th Circuit (2005), the U.S. Court of Appeals—7th Circuit (2011), the U.S. Court of Appeals—9th Circuit (2011), and the U.S. Court of Appeals—D.C. Circuit (1991).

4. I have taught Information Privacy Law continuously at Georgetown University Law Center since 1990.

5. I am co-author with Anita Allen of a leading casebook on privacy law.

6. In my capacity as President and Executive Director, I have supervised both EPIC's response to the Department's rulemaking and EPIC'S participation in all stages of litigation in the above-captioned matter.

7. The statements contained in this declaration are based on my own personal knowledge.

8. EPIC works with an Advisory Board consisting of nearly 100 experts from across the United States drawn from the information law, computer science, civil liberties and privacy communities.

9. Members of the EPIC Advisory Board must formally commit to joining the organization and to supporting the mission of the organization.

10. Members of the EPIC Advisory Board make financial contributions to support the work of the organization.

11. Members of the EPIC Advisory Board routinely assist with EPIC's substantive work. For example, members provide advice on EPIC's projects, speak at EPIC conferences, and sign on to EPIC amicus briefs.

12. In this matter, EPIC represented the interests of more than 30 members of the EPIC Advisory Board, who signed a Statement to the National Association of State Secretaries in Opposition to the Commission's demand for personal voter data.

Under penalty of perjury, I declare that the foregoing is true and correct to the best of my knowledge and belief.

Marc Rotenberg
EPIC President and Executive Director

Executed this 7th day of July, 2017

U.S. General Services Administration

Privacy Impact Assessments (PIA)

GSA collects, maintains and uses personal information on individuals to carry out the agency's mission and responsibilities and to provide services to the public. By federal law and regulation, privacy issues and protections must be considered for information technology systems that contain any personally identifiable information. GSA uses the Privacy Impact Assessment (PIA) as a key tool in fulfilling these legal and regulatory obligations. By conducting PIAs, GSA ensures that:

- The information collected is used only for the intended purpose;
- The information is timely and accurate;
- The information is protected according to applicable laws and regulations while in GSA's possession;
- The impact of the information systems on individual privacy is fully addressed; and
- The public is aware of the information GSA collects and how the information is used.

PIA Systems

System Title	Acronym/Short Name
ACMIS	ACMIS [PDF - 222 KB]
Challenge.gov	Challenge.gov [DOC - 206 KB]
Childcare Subsidy	CCS [PDF - 329 KB]
Citizen Engagement Platform	CEP [DOC - 100 KB]
ClearPath Hosting Services	GSA FSS-13 [PDF - 189 KB]
Controlled Document Tracker	CDT [PDF - 107 KB]
Customer Engagement Organization	CEO [DOC - 120 KB]
Data.gov	Data.gov [PDF - 300 KB]
Data Leakage Prevention	DLP [PDF - 173 KB]
Digital.gov	Digital.gov [PDF - 474 KB]
eGOV Jobcenter	eGOV Jobcenter [PDF - 199 KB]
eLease	eLease [PDF - 144 KB]
Electronic Acquisition System - Comprizon	EAS-Comprizon [PDF - 158 KB]
Electronic Document Management Software	EDMS [PDF - 49 KB]
EMD	EMD [PDF - 202 KB]
E-PACS	E-PACS [PDF - 48 KB]
E-Travel Carlson Wagonlit Government Travel E2 Solutions	E2Solutions [PDF - 174 KB]
E-Travel Northrop Grumman Mission Solutions - GovTrip	E-Travel GovTrip [PDF - 227 KB]
FAI On-Line University	FAI [PDF - 113 KB]
FAR Data Collection Pilot	FAR [PDF - 51 KB]
FBO	FBO [PDF - 489 KB]
Federal Personal Identity Verification Identity Management System	PIV IDMS [PDF - 222 KB]
ImageNow	ImageNow [PDF - 145 KB]
JP Morgan Chase	JP Morgan [PDF - 55 KB]
Login.gov	Login.gov [PDF - 196 KB]
National Contact Center (NCC)	NCC [PDF - 172 KB]
Office of Inspector General Information System	OIGMIS [PDF - 161 KB]
Office of Inspector General Counsel Files	GSA/ADM-26 [DOC - 38 KB]

System Title	Acronym/Short Name
OGC Case Tracking	OGC [PDF - 3 KB]
Open Government Citizen Engagement Tool	OGC Engagement [PDF - 384 KB]
ORC	ORC [PDF - 211 KB]
Payroll Accounting and Reporting (PAR)	PAR [PDF - 245 KB]
Pegasys	Pegasys [PDF - 54 KB]
PPFM 8 Chris	PPFM 8 [PDF - 65 KB]
Sales Automation System	SASy [DOC - 104 KB]
Social Media Platforms	Social Media [PDF - 84 KB]
STAR	STAR [DOC - 259 KB]
System for Award Management (SAM)	SAM [DOC - 39 KB]
The Museum System	TMS [PDF - 141 KB]
Transit	Transit [PDF - 195 KB]
USA.gov	USA.gov [PDF - 424 KB]
USAccess	USAccess [PDF - 240 KB]

CONTACTS

GSA Privacy Act Officer

- View Contact Details

PIA POLICY

- 1878.2A CIO P - Conducting Privacy Impact Assessments (PIAs) in GSA

PIA TEMPLATES

- PIA Template
- PIA template for Agency Use of Third-Party Websites and Applications

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 1:17-cv-1320 (CKK)

DECLARATION OF CHARLES CHRISTOPHER HERNDON

I, Charles C. Herndon, declare as follows:

1. I am the Director of White House Information Technology ("WHIT") and Deputy Assistant to the President. I am the senior officer responsible for the information resources and information systems provided to the President, Vice President and Executive Office of the President. I report to White House Deputy Chief of Staff for Operations and Assistant to the President, and through him to the Chief of Staff and the President. I am part of what is known as the White House Office. This declaration is based on my personal knowledge and upon information provided to me in my official capacity.

2. A number of components make up the Executive Office of the President, including the White House Office (also referred to as the Office of the President). Components of the White House Office include the President's immediate staff, the White House Counsel's Office and the Staff Secretary's Office. The White House Office serves the President in the performance of the many detailed activities incident to his immediate office, and the various

Assistants and Deputy Assistants to the President aid the President in such matters as he may direct. My role is to ensure the effective use of information resources and systems to the President. I am also a member of the Executive Committee for Presidential Information Technology, as established in the March 19, 2015, Presidential Memorandum creating my position. See, https://obamawhitehouse.archives.gov/the-press-office/2015/03/19/presidential-memorandum-establishing-director-white-house-information-te. The Executive Committee is chaired by the Deputy Chief of Staff Operations.

3. I was asked by the Office of the Vice President to assist in creating a mechanism by which data could be securely loaded and stored within the White House computer systems. To do that I repurposed an existing system that regularly accepts personally identifiable information through a secure, encrypted computer application within the White House Information Technology system.

4. States that wish to provide information to the Presidential Advisory Commission on Election Integrity ("Commission") can email the Commission to request an access link. Once a staff member verifies the identity of the requester and the email address, a one-time unique uniform resource locator ("URL") link will be emailed to that state representative. Data can be uploaded via that one-time link to a server within the domain electionintegrity.whitehouse.gov. Authorized members of the Commission will be given access to the file directory identified to house the uploaded information. Once the files have been uploaded, there is no further transfer of the data from that location. The technology is similar to a shared folder in Microsoft SharePoint.

5. The Commission will receive dedicated laptops, which can access the data provided by states through the White House network over an SSL (Secure Sockets Layer)

connection. The SSL connection ensures that all data passed between the web server and browsers remain private and secure. The laptops use Personal Identity Verification (PIV) and the data at rest is encrypted.

6. The Executive Committee for Information Technology will have no role in this data collection process. The U.S. Digital Service (which is within the Office of Management and Budget) will also have no role, nor will any federal agency. The only people who will assist are a limited number of my technical staff from the White House Office of Administration. They will have access to the data, but all access will be logged and recorded by our network monitoring tools.

7. I can confirm, based on information provided to me from the Department of Defense, that the data the state of Arkansas uploaded to the Army's SAFE site has been deleted without ever having been accessed by the Commission.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

***

Executed this 16th day of July 2017.

Digitally signed by CHARLES HERNDON
DN: c=US, o=U.S. Government, ou=Executive Office of the President, cn=CHARLES HERNDON, 0.9.2342.19200300.100.1.1=11001003426249
Date: 2017.07.17 06:36:16 -04'00'

Charles C. Herndon

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY; MICHAEL PENCE, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; KRIS KOBACH, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES; OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES; GENERAL SERVICES ADMINISTRATION Defendants.	Civ. Action No. 17-1320 (CKK)

DECLARATION BY ELENI KYRIAKIDES

I, Eleni Kyriakides, declare as follows:

1. My name is Eleni Kyriakides.

2. I am an EPIC Law Fellow at the Electronic Privacy Information Center.

3. In my capacity as a Fellow, I coordinate EPIC's Open Government Project. This includes overseeing EPIC's work using the Freedom of Information Act (FOIA).

4. EPIC makes frequent use of the FOIA to obtain records on government programs implicating privacy and civil liberties. EPIC seeks public disclosure of this information to help ensure that the public is fully informed about the activities of government, and to conduct oversight and analysis of these programs.

5. By refusing to release a Privacy Impact Assessment as required by law, the Defendants have increased the burden on EPIC to conduct its "oversight and analysis" in a more costly and resource-intensive way that would not otherwise be necessary.

6. As a result, I have researched, drafted, and submitted five requests seeking details related to the Commission's recent activities: one to the U.S. Department of Justice, two to the Commission, one to the General Services Administration, and one to the Arkansas Secretary of State Mark Martin. *See* EPIC Exhibit FOIA Requests.

I declare under penalty of perjury that, to the best of my knowledge, the forgoing is true and correct.

Executed July 17, 2017.

Respectfully Submitted,

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: July 17, 2017

epic.org
Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA
+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA E-MAIL

June 30, 2017

Nelson D. Hermilla, Chief
FOIA/PA Branch
Civil Rights Division
Department of Justice
BICN Bldg., Room 3234
950 Pennsylvania Avenue, NW
Washington, DC 20530
CRT.FOIArequests@usdoj.gov

Dear Mr. Hermilla,

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Department of Justice ("DOJ").

On June 28, 2017, the DOJ wrote to all states covered by the National Voter Registration Act ("NVRA") with a sweeping request for information regarding state voter registration list maintenance including "All statutes, regulations, written guidance, internal policies, or database user manuals that set out the procedures" the states have in place related to voter registration requirements, any other relevant procedures, and an explanation of the officials responsible for maintaining voter registration lists. The DOJ also sought, for local election officials, descriptions of the steps taken to ensure list maintenance is in "full compliance with the NVRA."[1] The DOJ gave the states 30 days to comply with the request. The DOJ offered no explanation or justification for the unprecedented time-bound request, stating only that the agency "reviewing voter registration list maintenance procedures in each state covered by the NVRA."[2]

Also on June 28, 2017, the Kris Kobach, the Vice Chair of the Presidential Advisory Commission on Election Integrity ("PACIE"), sent a letter to the Secretaries of State for all 50 states and the District of Columbia asking that the states provide the Commission detailed voter information, including

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony

[1] *See, e.g.*, Letter from T. Christian Herren, Jr., Chief, Voting Section, U.S. Dep't ment of Justice, to Kim Westbrook Strach, Exec. Dir., North Carolina State Bd. Of Elections (June 28, 2017), https://www.documentcloud.org/documents/3881855-Correspondence-DOJ-Letter-06282017.html.
[2] *Id.*

convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.[3]

EPIC seeks two categories of records concerning the DOJ's June 28th request for information on state voter list procedures.

Records Requested

(1) All records, including memoranda, legal analyses, and communications, concerning the DOJ's June 28, 2017 request to the states regarding voter list maintenance; and

(2) All communications between the DOJ and the Presidential Advisory Commission on Election Integrity ("PACEI") regarding the June 28, 2017 PACEI request for state voter data as well as any legal memoranda concerning the authorities of the PACEI.

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request. 5 U.S.C. § 552(a)(6)(E)(v)(II). To warrant expedited processing, under DOJ FOIA regulations a FOIA request must concern a matter of (1) "urgency to inform the public about an actual or alleged federal government activity," and, (2) the request must be "made by a person who is primarily engaged in disseminating information." 28 C.F.R. § 16.5(e)(1)(ii). This request satisfies both requirements.

First, there is an "urgency to inform the public about an actual or alleged federal government activity." § 16.5(e)(1)(ii). The "actual…federal government activity" at issue is DOJ's request to the states covered by the National Voter Registration Act ("NVRA") for information concerning each state's "voter registration list maintenance procedures." The DOJ concedes this activity in letters to the states.[4]

"Urgency" to inform the public about this activity is clear given the extraordinary nature and unusual breadth of the DOJ's request. On June 28, 2017, DOJ requested that all states covered by the NVRA provide to the DOJ *within 30 days* a sweeping list of information about state voting list maintenance. Indeed, former DOJ civil rights official and professor Justin Levitt told *ProPublica* that "he did not recall a time when the DOJ has previously requested such broad information."[5] Former senior litigator with the DOJ's Voting Section, David Becker called the move "unprecedented":

---

[3] *See, e.g.* Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html; *See generally* EPIC, *Voter Privacy and the PACEI,* https://epic.org/privacy/voting/pacei/.

[4] *Id.*

[5] *Jessica Huseman, Presidential Commission Demands Massive Amounts of State Voter Data,* ProPublica (June 29, 2107), https://www.propublica.org/article/presidential-commission-demands-massive-amounts-of-state-voter-data.

> In the quarter-century since passage of the NVRA, of which I spent seven years as a DOJ lawyer enforcing the NVRA, among other laws, *I do not know of the DOJ conducting any other broad-based fishing expedition into list maintenance compliance, whether during Democratic or Republican administrations*.[6]

Former deputy assistant general for civil rights Sam Bagnestos warned: "Let's be clear about what this letter signals: DOJ Civil Rights is preparing to sue states to force them to trim their voting rolls."[7]

The DOJ's request also represents a selective review of state voting processes,[8] without any basis offered for its narrow focus. The NVRA was passed not only to ensure "accurate and current voter registration rolls," but also "to establish procedures that will increase the number of eligible citizens who register to vote in elections for Federal office" and recognized that "the right of citizens of the United States to vote is a fundamental right." 52 U.S.C. § 20501. For instance, the DOJ request did not include an information request for compliance NVRA requirements voter registration forms be made easily available for distribution (§ 20505(b)), for simultaneous voter registration while applying for a driver's license (§ 20505(a)), and that state offices that provide public assistance and services to those with disabilities provide voter registration application forms and assistance (§ 20505(a)(4)(A)).

Despite the extraordinary nature of the request the DOJ offered no explanation or justification for the sudden broad-based request. The DOJ merely cited an agency review of "voter registration list maintenance procedures" in these states,[9] and "did not respond to requests for comment about the letters."[10]

States have thirty days to respond to the DOJ request. There is an urgent public need for immediate release of information explaining the DOJ's unprecedented decision to demand this voting list information from states. Moreover, the coincidental request by the PACEI for similar information from the states raises substantial concerns that the DOJ request was part of a coordinated undertaking. The PACEI has given the states approximately two weeks to respond their request.

Second, EPIC is an organization "primarily engaged in disseminating information." § 16.5(e)(1)(ii). As the Court explained in *EPIC v. Dep't of Def.*, "EPIC satisfies the definition of

---

[6] David Becker, *Why Wednesday's 'Election Integrity' Actions Should Be Watched By States*, Route Fifty (June 29, 2017), http://www.routefifty.com/management/2017/06/trump-election-integrity-commission-state-voter-data/139107/ (emphasis added).
[7] @sbagen, Twitter (June 29, 2017, 1:46 PM), https://twitter.com/sbagen/status/880528035392491520.
[8] *Jessica Huseman*, *supra* note 6.
[9] *See* Letter from T. Christian Herren, Jr. to Kim Westbrook Strach, Exec. Dir., North Carolina State Bd. Of Elections, *supra* note 1.
[10] *Id.*

'representative of the news media'" entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because disclosure of the requested information "is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest" of EPIC. 28 C.F.R. § 16.10(k)(1); § 552(a)(4)(A)(iii). EPIC's request satisfies the FBI's three factors for granting a fee waiver. § 16.10(k)(2).

Under the DOJ FOIA regulations, DOJ components evaluate three considerations to determine whether fee waiver is warranted: (i) the "subject of the request must concern identifiable operations or activities of the Federal Government with a connection that is direct and clear, not remote or attenuated"; (ii) disclosure must be "likely to contribute significantly to public understanding of those operations or activities"; and (iii) "disclosure must not be primarily in the commercial interest of the requester." §§ 16.10(k)(2)(i)–(iii).

First, disclosure of the requested DOJ records concerning the June 28th request to states for "voter registration list maintenance" self-evidently "concerns identifiable operations or activities of the Federal Government with a connection that is direct and clear, not remote or attenuated." § 16.10(k)(2)(i). This request concerns a direct request from the DOJ to states for information, concerning a law that the DOJ is authorized to enforce.

Second, disclosure "would be likely to contribute significantly to public understanding of those operations or activities" according to the two sub-factors. § 16.10(k)(2)(ii)(A-B). As to the first sub-factor, disclosure would be "meaningfully informative about government operations or activities" because the justification and decision-making underlying for the DOJ's unprecedented request to states covered by the NVRA has not been made public. § 16.10(k)(2)(ii)(A). Any additional information about how why the DOJ is seeking broad based data under only select provisions of NVRA would thus be "meaningfully informative" about the DOJ request. As to the second sub-factor, disclosure will "contribute to the understanding of a reasonably broad audience of persons interested in the subject," because, as stated in the relevant FOIA regulations, components will "presume that a representative of the news media will satisfy this consideration." § 16.10(k)(2)(ii)(B).

Third, disclosure of the requested information is not "primarily in the commercial interest" of EPIC according to the two sub-factors. § 16.10(k)(2)(iii)(A-B). As to the first sub-factor, EPIC

has no "commercial interest…that would be furthered by the requested disclosure." § 16.10(k)(2)(iii)(A). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[11] As to the second sub-factor, "the component must determine whether that is the primary interest furthered by the request" because, as stated in the FOIA regulations, DOJ "ordinarily will presume that where a news media requester has satisfied [the public interest standard], the request is not primarily in the commercial interest of the requester." § 16.10(k)(2)(iii)(B). As already described above, EPIC is a news media requester and satisfies the public interest standard.

For these reasons, a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. I anticipate your determination on our request within ten calendar days 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

[11] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.

epic.org
Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA
+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA E-Mail

July 4, 2017
Presidential Advisory Commission on Election Integrity
ElectionIntegrityStaff@ovp.eop.gov

Dear Sir or Madam:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Presidential Commission on Election Integrity ("PACEI" or "Commission").

This is a request for records in possession of the agency concerning the letters that were sent on or about June 28, 2017 requesting the production of state voter records and other related information.

Background

The Presidential Advisory Commission on Election Integrity was established by executive order on May 11, 2017.[1] On June 28, 2017, the Commission undertook an effort to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.[2]

The Vice Chair indicated that the Commission expected a response from the states by July 14, 2017.[3]

Such a request to state election officials had never been made by any federal official before. Election officials across the political spectrum in at least two dozen states have already partially or fully refused to comply with PACEI's request.[4]

---

[1] Exec. Order No. 13,799, 82 Fed. Reg. 22, 389 (May 11, 2017).
[2] Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Sec'y of State, North Carolina (June 28, 2017), https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html.
[3] *Id.*
[4] Philip Bump & Christopher Ingraham, *Trump Says States Are 'Trying to Hide' Things from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017),

On June 28th, the U.S. Department of Justice issued a parallel request. The DOJ wrote to all states covered by the National Voter Registration Act with a similarly unprecedented demand for information regarding compliance with state voter registration list maintenance.[5] The DOJ gave the states 30 days to comply with the request.

EPIC seeks nine categories of records from the agency concerning the Commission's June 28th, 2017 request to state election officials.

Records Requested

(1) All communications to state election officials regarding the request;

(2) All communications between and amongst Commission staff and Commission members regarding the request;

(3) All communications between the Commission staff and the Department of Justice and all communications between Commission members and the Department of Justice regarding the request;

(4) All records concerning compliance with the E-Government Act of 2002 and the specific obligation to undertake a Privacy Impact Assessment;

(5) All records concerning compliance with the Federal Advisory Committee Act and the failure to post a Privacy Impact Assessment;

(6) All records concerning compliance with the Privacy Act of 1974 and the failure to undertake a Systems of Records Notice;

(7) All records concerning the decision to use an insecure website and an insecure email address to receive state voter data;

(8) All legal memorandum concerning the Commission's authority to request personal data from the states; and

(9) Such other records that assess the privacy and security risks of aggregating nearly two hundred million voter records in a federal database.

---

https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/?utm_term=.bd2ba9587f57.

[5] *See, e.g.*, Letter from T. Christian Herren, Jr., Chief, Voting Section, U.S. Dep't ment of Justice, to Kim Westbrook Strach, Exec. Dir., North Carolina State Bd. Of Elections (June 28, 2017), https://www.documentcloud.org/documents/3881855-Correspondence-DOJ-Letter-06282017.html.

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request. To warrant expedited processing, a FOIA request must concern a "compelling need." 5 U.S.C. § 552(a)(6)(E)(i). "Compelling need" is demonstrated where the request is (1) "made by a person primarily engaged in disseminating information," with (2) "urgency to inform the public concerning actual or alleged Federal Government activity." § 552(a)(6)(E)(v)(II). This request satisfies both requirements.

First, EPIC is an organization "primarily engaged in disseminating information." § 552(a)(6)(E)(v)(II). As the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media.'" 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

Second, there is an "urgency to inform the public about an actual or alleged Federal Government activity." § 552(a)(6)(E)(v)(II). The "actual…Federal Government activity" at issue is PACEI's request to states for detailed voter history information. The PACEI concedes this activity in letters to the states.[6]

"Urgency" to inform the public about this activity is clear given the extraordinary nature of PACEI's sweeping request for voter data.[7] On June 28, 2017, PACEI independently requested that fifty states and D.C. - within approximately *ten business days* – disclose sensitive, personal information that individuals are often required to provide to be eligible to vote. To date, PACEI has not indicated how the information will be used, who will have access to it, or what safeguards will be established. PACEI has also not made any Privacy Impact Assessment for the collection of state voter data.

As noted already, state officials in over two dozen states have partially or fully opposed PACEI's demand.[8] Mississippi Secretary of State Delbert Hosemann stated, "They can go jump in the Gulf of Mexico."[9] California Secretary of State Alex Padilla added that he would "not provide sensitive voter information to a committee that has already inaccurately passed judgment that millions of Californians voted illegally. California's participation would only serve to legitimize the false and already debunked claims of massive voter fraud."[10] Kentucky's Secretary of State

---

[6] *See* Letter from Kris Kobach to Elaine Marshall, *supra* note 2.
[7] *Voter Privacy and the PACEI*, Epic.org, https://epic.org/privacy/voting/pacei/.
[8] *See* Philip Bump & Christopher Ingraham, *supra* note 4.
[9] Editorial Board, *Happy Fourth of July! Show Us Your Papers*, N.Y. Times (July 3, 2017), https://mobile.nytimes.com/2017/07/03/opinion/voter-fraud-data-kris-kobach.html.
[10] Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017), http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/.

Alison Lundergan Grimes concluded, "There's not enough bourbon here in Kentucky to make this request seem sensible."[11]

Fifty technical experts and legal scholars and twenty organizations expert in election integrity, voting verification, and voter privacy also recorded opposition to PACEI's request. In a letter to state officials, they explained: "As custodians of voter data, you have a specific responsibility to safeguard voter record information."[12]

This request concerns a matter of widespread public concern; the right to vote is protected by the U.S. Constitution. U.S. Const. amends. XV, XIX, XXIV, XXVI. Voter privacy and the secret ballot are unquestionably integral to American democracy.

States have only days left to respond to PACEI's request. There is an urgent public need for immediate release of information explaining the PACEI's unprecedented decision to collect, en masse, voters' personal information from the states. Moreover, the coincidental request by the DOJ for similar information from the states raises substantial concerns that the PACEI request was part of a coordinated undertaking.[13]

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because disclosure of the requested information "is in the public interest" because (1) "it is likely to contribute significantly to public understanding of the operations or activities of the government," and (2) disclosure "is not primarily in the commercial interest" of EPIC. § 552(a)(4)(A)(iii).

First, disclosure of the requested PACEI records concerning the June 28th request to states for detailed voter histories "is likely to contribute significantly to public understanding of the operations or activities of the government." § 552(a)(4)(A)(iii). The requested PACEI records self-evidently concerns "operations or activities of the government." *Id.* This request concerns a direct

---

[11] Max Greenwood, *Kentucky secretary of state: 'Not enough bourbon in Kentucky' to make me release voter data*, Hill (June 30, 2017), http://thehill.com/homenews/state-watch/340331-kentucky-secretary-of-state-not-enough-bourbon-in-kentucky-to-make-me.
[12] Letter from Organizations and Individual Experts to National Association of State Secretaries (July 3, 2017), https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf.
[13] *See* Letter from Eleni Kyriakides, EPIC Law Fellow, to Nelson Hermilla, Chief, FOIA/PA Branch, Civil Rights Div. (June 30, 2017), https://epic.org/privacy/voting/EPIC-17-06-30-DOJ-20170630-Request.pdf

request from a presidential commission to state officials to obtain state voter information. Disclosure of the PACEI records is also "likely to contribute significantly to public understanding" of the Commission's activities because, despite the extraordinary nature of PACEI's demand, the Commission has not explained how it plans to use, protect, or dispose of the sensitive personal data requested. § 552(a)(4)(A)(iii). Any additional information about how and why PACEI is seeking this data would "contribute significantly" to the public's understanding of PACEI's activities.

Second, disclosure of the requested information is not "primarily in the commercial interest" of EPIC. § 552(a)(4)(A)(iii). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[14]

For these reasons, a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. I anticipate your determination on our request within ten calendar days 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

[14] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.

epic.org
Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA
+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA MAIL & FOIAonline

June 12, 2017

U.S. General Services Administration
FOIA Requester Service Center (H1F)
1800 F Street, NW, Room 7308
Washington, DC 20405-0001

Dear Sir/Madam,

This letter constitutes an urgent request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the General Services Administration ("GSA").

EPIC seeks records in possession of the agency concerning the transfer of voter data from the State of Arkansas to the Department of Defense following the June 28, 2017 letter from the Presidential Advisory Commission on Election Integrity (the "Commission").

Background

On June 28, 2017, the Vice Chair of the Commission attempted to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information. [1]

The letter provides no indication that the Commission will pay fees for the receipt voter data. The Commission also indicated a website for the transmission of voter data, which has since been determined to be insecure for the receipt of personally identifiable information from the general public.[2] Further, the letter from the Commission indicated no familiarity with the data that may disclosed by a particular state that received the request or the procedures the Commission would be required to follow to obtain voter data from a particular state.

---

[1] *See, e.g.* Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html.

[2] Lewis Decl. Ex. 11., EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

Following a proceeding brought by EPIC, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017) on July 7, 2017 the U.S. Department of Justice told the D.C. District Court that Arkansas transferred voter data, to the Department of Defense's SAFE Website, following the letter from the Vice Chair.[3]

The Arkansas Secretary of State's Office charges $2.50 per statewide voter registration data file.[4] A requesting party also completes a "Data Request Form" in order to obtain the file and must mail payment (in check or money order form) to the Arkansas Secretary of State offices.[5] The Office provides three types of files, with three clearly defined sets of information:

> (1) "…Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted."
>
> (2) "Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle" while "older elections are incomplete since some counties did not enter voter results into the previously used VR databases." And
>
> (3) "…a combination of the Voter Registration and Vote History files (VRVH)."[6]

The files are provided in ".CSV format" and "are available in CD format for pickup at the State Capitol Building or by mail" or "can also be placed on an FTP site."[7]

EPIC seeks four categories of records from the agency concerning the Arkansas transfer of data to the Commission.

Records Requested

> (1) All records indicating payment by the Commission to obtain Arkansas voter records;
>
> (2) The completed "Data Request Forms," prepared by the Commission to obtain the Arkansas state vote records;
>
> (3) All records indicating the types of data transferred by Arkansas to the Commission; and

---

[3] Transcript of Temporary Restraining Order at 40, EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).
[4] *Voter Data Request Form*, Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/Data%20Request%20Form.pdf (last visited July 12, 2017).
[5] *Id.*
[6] *Id.*
[7] *Id.*

(4) All records indicating the Commission's compliance with the Arkansas procedures to obtain state voter records.

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request because this request involves a "compelling need." 5 U.S.C. § 552(a)(6)(E)(i). Specifically, under GSA FOIA regulations a request warrants expedited processing where the information sought is (1) "urgently needed," (2) "by an individual primarily engaged in disseminating information," and (3) "in order to inform the public concerning actual or alleged Federal Government activity." 41 C.F.R. § 105-60.402-2(c)(2). This request satisfies all three requirements.

First, records concerning the Arkansas voter data transfer to the SAFE website, obtained following the June 28th request, is "urgently needed." § 105-60.402-2(c)(2). This information "has a particular value that will be lost if not disseminated quickly." *Id.* Indeed, this request concerns *both* a "breaking news story" and an issue of significant "general public interest." *Id.* On June 28, 2017, PACEI independently requested that fifty states and D.C. - within approximately *ten business days* – disclose sensitive, personal information individuals are often required to provide to be eligible to vote. Since that date, public interest in the PACEI's demand for state election officials to transfer personal voter data has dominated the news cycle, driven by prompt dissent of state officials in at least two dozen states across the political spectrum and public outcry.[8] Following PACEI's request less than two weeks ago, "[t]en states noted at least a slight increase in citizen calls and emails, and some citizens inquired about the process to unregister to vote, or how to secure their personal information."[9]

On July 7th, in a hearing before the D.C. District Court, the DOJ first revealed that Arkansas alone had transferred personal data to the Commission.[10] There are approximately 1.7 million registered voters in the state of Arkansas potentially implicated by this transfer.[11] The Commission will hold its first meeting on July 19, 2017.[12] Ahead of that meeting, the public must know whether the Commission and Arkansas state officials complied with state procedures in transferring this sensitive personal data.

---

[8] Philip Bump & Christopher Ingraham, *Trump Says States Are 'Trying to Hide' Things from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/?utm_term=.bd2ba9587f57.

[9] Dylan Wells & Saisha Talwar, *Some voters un-registering following Trump administration's data requests*, ABC News (July 11, 2017), http://abcnews.go.com/Politics/voters-registering-trump-administrations-data-requests/story?id=48578555.

[10] Transcript of Temporary Restraining Order at 40, *supra* note 3.

[11] *Registered Voters [As of 6/1/16]*, Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/ARRegisteredVoters6-1-16.pdf (last visited July 12, 2017).

[12] Meeting notice, 82 FR 31063 (July 5, 2017).

Second, EPIC is an organization "primarily engaged in disseminating information," § 105-60.402-2(c)(2). As the Court explained in *EPIC v. Dep't of Def.*, "EPIC satisfies the definition of 'representative of the news media'" entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

Third, this request involves "actual…federal government activity." § 105-60.402-2(c)(2). This FOIA concerns PACEI's request to states for detailed voter history information, conceded by PACEI in letters to the states,[13] and the transfer of Arkansas voter data to PACEI via the SAFE website, conceded by the DOJ to the D.C. District Court.[14]

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 105-60.402-2(c); § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II); 41 C.F.R. § 105-60.305-10(d)(2).

Further, any duplication fees should also be waived because disclosure of the requested information "would contribute significantly to public's understanding of the operations or activities of the Government and would not be primarily in the commercial interest" of EPIC. § 105-60.305-13; § 552(a)(4)(A)(iii). The GSA evaluates four considerations to determine whether this standard is met: (1) "Whether the subject of the requested records concerns 'the operations or activities of the Government,'"(2) "Whether the disclosure is 'likely to contribute' to an understanding of Government operations or activities," (3) "Whether disclosure of the requested information will contribute to [the] 'public's understanding,'" and (4) "Whether the requester has a commercial interest that would be furthered by the requested disclosure; and if so: whether the magnitude of the identified commercial interest of the requester is sufficiently large, in comparison with the public's interest in disclosure, that disclosure is 'primarily in the commercial interest of the requester.'" § 105-60.305-13(a)(1-4). EPIC's request satisfies these four GSA considerations for granting a fee waiver. § 105-60.305-13(a)(1-4).

First, disclosure of the requested GSA records concerning Arkansas transfer of voter data following PACEI's June 28th request self-evidently concerns "the operations or activities of the Government." § 105-60.305-13(a)(1). This request involves a direct request from a presidential commission to a state officials to obtain state voter information, and the transfer of data to a federal website following that request.

Second, "disclosure is 'likely to contribute' to an understanding of Government operations or activities." § 105-60.305-13(a)(2). The requested information about the Arkansas data transfer is

[13] *See* Letter from Kris Kobach to Elaine Marshall, *supra* note 1.
[14] Transcript of Temporary Restraining Order at 40, *supra* note 3.

not "already in the public domain." *Id.* Few details surrounding the transfer have been disclosed to the public, and the existence of the transfer was first made public mere days ago.

Third, "disclosure of the requested information will contribute to [the] 'public's understanding" § 105-60.305-13(a)(3). As stated in the GSA FOIA regulations, the "identity and qualifications of the requester should be considered to determine whether the requester is in a position to contribute to public's understanding through the requested disclosure." *Id.* As already indicated, EPIC is a news media requester. EPIC regularly disseminates information obtained through the FOIA as a part of its public interest mission through website EPIC.org, a bi-weekly "EPIC Alert," and other publications.[15]

Fourth, EPIC has no "commercial interest that would be furthered by the requested disclosure." § 105-60.305-13(a)(4). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[16]

For these reasons, a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. I anticipate your decision concerning EPIC's request for expedited processing within five working days. 41 C.F.R. § 105-60.402-2(d). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

[15] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.
[16] *Id.*

epic.org
Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA
+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA E-Mail

July 12, 2017
Presidential Advisory Commission on Election Integrity
ElectionIntegrityStaff@ovp.eop.gov

Dear Sir or Madam:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Presidential Commission on Election Integrity (the "Commission").

EPIC seeks records in possession of the agency concerning the transfer of voter data from the State of Arkansas to the Department of Defense following the June 28, 2017 Commission letter.

Background

On June 28, 2017, the Vice Chair of the Commission attempted to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information. [1]

The letter provides no indication that the Commission will pay fees for the receipt voter data. The Commission also indicated a website for the transmission of voter data, which has since been determined to be insecure for the receipt of personally identifiable information from the general public.[2] Further, the letter from the Commission indicated no familiarity with the data that may disclosed by a particular state that received the request or the procedures the Commission would be required to follow to obtain voter data from a particular state.

Following the proceeding brought by EPIC, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017) on July 7, 2017 the U.S. Department of Justice told the D.C. District Court that

---

[1] *See, e.g.* Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html.

[2] Lewis Decl. Ex. 11., EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

Arkansas transferred voter data, to the Department of Defense's SAFE Website, following the letter from the Vice Chair.[3]

The Arkansas Secretary of State's Office charges $2.50 per statewide voter registration data file.[4] A requesting party also completes a "Data Request Form" in order to obtain the file and must mail payment (in check or money order form) to the Arkansas Secretary of State offices.[5] The Office provides three types of files, with three clearly defined sets of information:

> (1) "…Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted."
>
> (2) "Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle" while "older elections are incomplete since some counties did not enter voter results into the previously used VR databases." And
>
> (3) "…a combination of the Voter Registration and Vote History files (VRVH)."[6]

The files are provided in ".CSV format" and "are available in CD format for pickup at the State Capitol Building or by mail" or "can also be placed on an FTP site."[7]

EPIC seeks four categories of records from the agency concerning the Arkansas transfer of data to the Commission.

Records Requested

> (1) All records indicating payment by the Commission to obtain Arkansas voter records;
>
> (2) The completed "Data Request Forms," prepared by the Commission to obtain the Arkansas state vote records;
>
> (3) All records indicating the types of data transferred by Arkansas to the Commission; and
>
> (4) All records indicating the Commission's compliance with the Arkansas procedures to obtain state voter records.

---

[3] Transcript of Temporary Restraining Order at 40, EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).
[4] *Arkansas Voter Registration Data*, Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/Data%20Request%20Form.pdf (last visited July 12, 2017).
[5] *Id.*
[6] *Id.*
[7] *Id.*

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request. To warrant expedited processing, a FOIA request must concern a "compelling need." 5 U.S.C. § 552(a)(6)(E)(i). "Compelling need" is demonstrated where the request is (1) "made by a person primarily engaged in disseminating information," with (2) "urgency to inform the public concerning actual or alleged Federal Government activity." § 552(a)(6)(E)(v)(II). This request satisfies both requirements.

First, EPIC is an organization "primarily engaged in disseminating information." § 552(a)(6)(E)(v)(II). As the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media.'" 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

Second, there is an "urgency to inform the public about an actual or alleged Federal Government activity." § 552(a)(6)(E)(v)(II). The "actual…Federal Government activity" at issue PACEI's request to states for detailed voter history information, conceded by PACEI in letters to the states,[8] and the transfer of Arkansas voter data to PACEI via the SAFE website, conceded by the DOJ in D.C. District Court.[9]

"Urgency" to inform the public about the Arkansas voter data transfer to the SAFE website, following the Commission's June 28th request. On June 28, 2017, PACEI independently requested that fifty states and D.C. - within approximately *ten business days* – disclose sensitive, personal information individuals are often required to provide to be eligible to vote. Since that date, public interest in the PACEI's demand for state election officials to transfer personal voter data has dominated the news cycle, driven by prompt dissent of state officials in at least two dozen states across the political spectrum and public outcry.[10] Following PACEI's request less than two weeks ago, "[t]en states noted at least a slight increase in citizen calls and emails, and some citizens inquired about the process to unregister to vote, or how to secure their personal information."[11]

On July 7th, in a hearing before the D.C. District Court, the DOJ first revealed that Arkansas alone had transferred personal data to the Commission.[12] There are approximately 1.7

---

[8] *See* Letter from Kris Kobach to Elaine Marshall, *supra* note 1.
[9] Transcript of Temporary Restraining Order at 40, *supra* note 3.
[10] Philip Bump & Christopher Ingraham, *Trump Says States Are 'Trying to Hide' Things from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/?utm_term=.bd2ba9587f57.
[11] Dylan Wells & Saisha Talwar, *Some voters un-registering following Trump administration's data requests*, ABC News (July 11, 2017), http://abcnews.go.com/Politics/voters-registering-trump-administrations-data-requests/story?id=48578555.
[12] Transcript of Temporary Restraining Order at 40, *supra* note 3.

million registered voters in the state of Arkansas potentially implicated by this transfer.[13] The Commission will hold its first meeting on July 19, 2017.[14] Ahead of that meeting, the public must know whether the Commission and Arkansas state officials complied with state procedures in transferring this sensitive personal data.

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because disclosure of the requested information "is in the public interest" because (1) "it is likely to contribute significantly to public understanding of the operations or activities of the government," and (2) disclosure "is not primarily in the commercial interest" of EPIC. § 552(a)(4)(A)(iii).

First, disclosure of the requested PACEI records concerning the Arkansas voter data transfer "is likely to contribute significantly to public understanding of the operations or activities of the government." § 552(a)(4)(A)(iii). The requested PACEI records self-evidently concerns "operations or activities of the government." *Id.* This request involves a direct request from a presidential commission to a state officials to obtain state voter information, and the transfer of data to a federal website following that request. Disclosure of the PACEI records is also "likely to contribute significantly to public understanding" of the Commission's activities because, the requested information about the Arkansas data transfer is not "already in the public domain." *Id.* Few details surrounding the transfer have been disclosed to the public. Indeed, the existence of the transfer was first made public mere days ago. Any additional information about the circumstances of the data transfer would there "contribute significantly" to the public's understanding of PACEI's activities. *Id.*

Second, disclosure of the requested information is not "primarily in the commercial interest" of EPIC. § 552(a)(4)(A)(iii). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[15]

For these reasons, a fee waiver should be granted.

---

[13] *Registered Voters [As of 6/1/16],* Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/ARRegisteredVoters6-1-16.pdf (last visited July 12, 2017).
[14] Meeting notice, 82 FR 31063 (July 5, 2017).
[15] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.

Conclusion

Thank you for your consideration of this request. I anticipate your decision concerning EPIC's request for expedited processing within ten calendar days. 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

epic.org
Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA
+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA MAIL

July 13, 2017

The Honorable Mark Martin
Secretary of State
ATTN: FOIA Officer
256 State Capitol
500 Woodlane Street
Little Rock, AR 72201

Dear Sir or Madam:

This letter constitutes a request under the Arkansas Freedom of Information Act Ark. Code Ann. § 25-19-105(a)(2)(A) (1967) to receive copies of records, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Office of Arkansas Secretary of State Mark Martin.

EPIC seeks records in possession of the Office concerning the transfer of voter data from the State of Arkansas to the Department of Defense following the June 28, 2017 Commission letter.

EPIC does not assert a claim to Arkansas records as a citizen of the state. § 25-19-105(a)(1)(A). Rather, EPIC urges the Secretary of State to publicly release the requested records in light of the profound public interest favoring release. "The generation that made the nation thought secrecy in government one of the instruments of Old World tyranny and committed itself to the principle that a democracy cannot function unless the people are permitted to know what their government is up to." *EPA v. Mink*, 410 U.S. 73, 105 (1973) (Douglas, W. dissenting) (quoting from The New York Review of Books, Oct. 5, 1972, p. 7). Transparency secures "informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). Here, EPIC seeks records concerning the Arkansas transfer of state voter data to the federal government in the pursuit of this overriding public interest.

Background

On June 28, 2017, the Vice Chair of the Commission attempted to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions,

information regarding voter registration in another state, information regarding military status, and overseas citizen information. [1]

The letter provides no indication that the Commission will pay fees for the receipt voter data. The Commission also indicated a website for the transmission of voter data, which has since been determined to be insecure for the receipt of personally identifiable information from the general public.[2] Further, the letter from the Commission indicated no familiarity with the data that may disclosed by a particular state that received the request or the procedures the Commission would be required to follow to obtain voter data from a particular state.

Following the proceeding brought by EPIC, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017) on July 7, 2017 the U.S. Department of Justice told the D.C. District Court that Arkansas transferred voter data, to the Department of Defense's SAFE Website, following the letter from the Vice Chair.[3]

The Arkansas Secretary of State's Office charges $2.50 per statewide voter registration data file.[4] A requesting party also completes a "Data Request Form" in order to obtain the file and must mail payment (in check or money order form) to the Arkansas Secretary of State offices.[5] The Office provides three types of files, with three clearly defined sets of information:

(1) "…Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted."

(2) "Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle" while "older elections are incomplete since some counties did not enter voter results into the previously used VR databases." And

(3) "…a combination of the Voter Registration and Vote History files (VRVH)."[6]

---

[1] *See, e.g.* Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html.

[2] Lewis Decl. Ex. 11., EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

[3] Transcript of Temporary Restraining Order at 40, EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

[4] *Arkansas Voter Registration Data*, Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/Data%20Request%20Form.pdf (last visited July 12, 2017).

[5] *Id.*

[6] *Id.*

The files are provided in ".CSV format" and "are available in CD format for pickup at the State Capitol Building or by mail" or "can also be placed on an FTP site."[7]

EPIC seeks four categories of records from the agency concerning the Arkansas transfer of data to the Commission.

Records Requested

(1) All records indicating payment by the Commission to obtain Arkansas voter records;

(2) The completed "Data Request Forms," prepared by the Commission to obtain the Arkansas state vote records;

(3) All records indicating the types of data transferred by Arkansas to the Commission; and

(4) All records indicating the Commission's compliance with the Arkansas procedures to obtain state voter records.

Request for Fee Waiver

EPIC requests that copies of the records "be furnished without charge or at a reduced charge" because (1) the records "have been requested primarily for noncommercial purposes," and (2) "waiver or reduction of the fee is in the public interest." § 25-19-105(d)(3)(A)(iv).

First, disclosure of the records "have been requested primarily for noncommercial purposes. § 25-19-105(d)(3)(A)(iv). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[8]

Second, "waiver or reduction of the fee is in the public interest." § 25-19-105(d)(3)(A)(iv). The requested records concern a matter of profound public interest: the transfer of Arkansas voters' data a Presidential commission. Nonetheless, there are few public details about the circumstances surrounding the transfer, and, indeed, the mere fact of the transfer was first made public only days ago.[9] On July 7th, in a hearing before the D.C. District Court, the DOJ first revealed that Arkansas alone had transferred personal data to the Commission.[10] There are approximately 1.7 million registered voters in the state of Arkansas potentially implicated by this transfer.[11] The Commission will hold its first meeting on July 19, 2017.[12] Ahead of that meeting,

---

[7] *Id.*
[8] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.
[9] Transcript of Temporary Restraining Order at 40, EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).
[10] *Id.*
[11] *Registered Voters [As of 6/1/16],* Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/ARRegisteredVoters6-1-16.pdf (last visited July 12, 2017).

the public must know whether the Commission and Arkansas state officials complied with state procedures in transferring this sensitive personal data.

For these reasons, a full fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org. EPIC anticipates your response within a maximum of three working days. § 25-19-105(e).

EPIC requests receipt of responsive records via e-mail, and, if not "readily convertible" to electronic format, in physical copies via mail to the 1718 Connecticut Ave. NW, Suite 200, Washington, DC 20009. § 25-19-105(d)(2)(B).

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

[12] Meeting notice, 82 FR 31063 (July 5, 2017).

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civ. Action No. 17-1320 (CKK)

PLAINTIFF'S AMENDED MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

Pursuant to the Court's July 11, 2017, Order and to Federal Rule of Civil Procedure 65 and LCvR 65.1, EPIC hereby moves this Court for a Temporary Restraining Order and Preliminary Injunction prohibiting Defendants from collecting voter roll data from state election officials prior to the completion and public release of a Privacy Impact Assessment as required by the E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note), and prior to the publication of a Federal Advisory Committee Act notice concerning the Privacy Impact Assessment, and prior to the resolution of EPIC's constitutional privacy claims.

The proposed collection and aggregation of state voter roll data by the Commission is without precedent. The Commission's pending action would place at risk the privacy of millions of registered voters—including military families and victims of stalking, whose home addresses would be revealed—and would undermine the integrity of the federal election system. Further, the request for partial Social Security Numbers that are often used as default passwords for commercial services, coupled with the Commission's plan to make voter records "publicly available," is both without precedent and crazy. The new facts that have come to light since

EPIC's original motion – including, (1) upon the Commission's instigation, the disclosure of Arkansas state voter records, contrary to state law and to a website not certified for personal information; (2) widespread concerns about the risks of the Commission's endeavor; and (3) the Commission stated intent to press on, pending this Court's decision -- underscore the need for injunctive relief.

This motion is supported by the attached Memorandum of Points and Authorities and exhibits, as well as the declarations and exhibits previously submitted,[1] and any additional submissions that may be considered by the Court.

Respectfully Submitted,

/s/ Marc Rotenberg
MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel

CAITRIONA FITZGERALD*
EPIC Policy Director

JERAMIE D. SCOTT, D.C. Bar # 1025909
EPIC Domestic Surveillance Project Director

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Plaintiff EPIC
** Pro hac vice motion pending*

Dated: July 13, 2017

[1] For the Court's convenience, attached to this motion are copies of all declarations and exhibits previously filed by EPIC in its motion, reply, and supplemental response.

18-F-1517//0867

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civ. Action No. 17-1320 (CKK)

MEMORANDUM IN SUPPORT OF PLAINTIFF'S AMENDED MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

18-F-1517//0868

TABLE OF CONTENTS

18-F-1517//0869

TABLE OF AUTHORITIES

Cases

18-F-1517//0870

Statutes

Other Authorities

18-F-1517//0871

18-F-1517//0872

INTRODUCTION

In the original emergency motion to this Court, EPIC explained that "the failure to safeguard personal data gathered by government agencies is a national crisis." EPIC pointed to the massive data breach at the Office of Personnel Management in 2015, and warned that the Commission's effort to gather state voter records, without regard for privacy, placed at risk the rights of millions of voters across this country. We respectfully asked this Court to issue a Temporary Restraining Order to enjoin the Commission from collecting state voter data.

Since EPIC filed the motion, there has been a substantial change in the factual record. The Commission went forward with its plan. It did not complete or publish a Privacy Impact Assessment. It did not publish a Federal Advisory Committee Act notice. It did not consider whether the extraordinary and unreasonable request for personal data without adequate privacy protection violated the constitutional right to privacy. It did not establish a method to securely receive personal data. It did not make any effort to work with the agency, the General Services Administration, designated in the Executive Order and the Commission Charter to provide "facilities," "equipment," and "administrative support" for the Commission. And it ignored calls from state election officials, experts in election system security, and twenty-four members of the United States Senate to end the program.

Further, upon the Commission's instigation, the State Secretary of Arkansas, over the objection of the Governor, turned over the state voter data to the Commission in violation of state law. No designation of appropriate data elements was made. No fees were received by the state. The state procedures for transferring state voter data were not followed. The Arkansas "Data Request Form" was never completed. The data was sent to a military website, designated by the Commission, that was not authorized to receive personal data from the general public.

Once these facts came to light, and upon the initiation of this litigation, the Commission did an about face. First, the Commission notified the states that it would suspend the data collection pending the Court's decision on this motion. Second, the Commission discontinued the

18-F-1517//0873

use of the military website to receive voter data. Third, the Commission stated it would delete the data that had been received from the state of Arkansas.

These are the events that have occurred since the filing of EPIC's initial complaint on July 3, 2017.

But the threat to voter privacy and democratic institutions remains. The Commission intends to move forward, pending this Court's determination. It has established a new server within the White House to receive the voter data. It has advised state election officials that further communications regarding this undertaking are forthcoming. But the Commission has given no indication that it will undertake a Privacy Impact Assessment, publish a FACA notice, or consider the Constitutional implications of this extraordinary request for personal data by the federal government. And the actual experience with the State of Arkansas makes clear that other states, by intent or inadvertence, may disclose to the Commission personal voter data, otherwise protected in law.

EPIC therefore respectfully renews its request for an injunction that would prohibit the Commission from collecting state voter record data pending resolution of this case. The requirements for an injunction are satisfied: (1) EPIC is likely to succeed on the merits of its claim; (2) EPIC and its members will be irreparably harmed; and (3) the balance of the equities and the public interest favors EPIC.

FACTUAL BACKGROUND

I. The Privacy Threat of Massive Voter Databases

Computer experts have long raised concerns about the collection of sensitive voter information in insecure databases. *E.g.*, Barbara Simons, *Voter Registration and Privacy* (2005);[1] EPIC, Comment Letter on U.S. Election Assistance Commission Proposed Information Collection Activity (Feb. 25, 2005).[2] Election officials "face many technical challenges in implementing [voter registration] databases in a secure, accurate, and reliable manner, while protecting sensitive

[1] https://epic.org/events/id/resources/simons.ppt.
[2] https://epic.org/privacy/voting/register/eac_comments_022505.html.

18-F-1517//0874

information and minimizing the risk of identity theft." Simons, *supra*, at 10. Voter registration databases "are complex systems," and "[i]t is likely that one or more aspects of the technology will fail at some point." Ass'n for Comput. Machinery, *Statewide Databases of Registered Voters: Study of Accuracy, Privacy, Usability, Security, and Reliability Issues* 6 (Feb. 2006), Ex. 26.[3] Moreover, merging data from multiple sources "can, if not properly handled, undermine the accuracy of the voter registration data." Simons, *supra*, at 12.

Recent events underscore the privacy risks inherent in assembling a nationwide voter database. In a recent hearing before the Senate Intelligence Committee, both federal and state election officials made clear that malicious hackers attack voter registration databases. *See Russian Interference in the 2016 U.S. Elections: Hearing Before the S. Select Comm. on Intelligence* (2017) (testimony of Jeanette Manfra, Acting Deputy Undersecretary for Cybersecurity & Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security) [hereinafter *SSCI 2016 Elections Hearing*], Ex. 27; *SSCI 2016 Elections Hearing* (testimony of Michael Haas, Administrator, Wisconsin Elections Commission), Ex. 28; *SSCI 2016 Elections Hearing* (statement of Hon. Connie Lawson, Secretary of State, Indiana), Ex. 29; *SSCI 2016 Elections Hearing* (statement of Steve Sandvoss, Executive Director, Illinois State Board of Elections), Ex. 30.

State officials recognize "the need for constantly enhancing the security of voter registration databases," especially due to the "confidential" nature of data held that can include "the voter's date of birth, the driver's license number, the last four digits of the social security number." *SSCI 2016 Elections Hearing* (transcript of panel 2), Ex. 32, at 4. The threats to state voter data are acute, and state officials have taken steps to keep that data secure within their own databases. For example, following the malicious cyber attack on the Illinois Voter Registration System database last year, the state began "introducing security enhancements" to their "web servers and databases." Ex. 30, at 1.

[3] https://people.eecs.berkeley.edu/~daw/papers/vrd-acm06.pdf.

18-F-1517//0875

States are well aware that "the 2016 elections reinforced the need for constantly enhancing the security of voter registration databases." Ex. 28, at 4. Already representatives from 27 states have joined an "Election Cybersecurity Task Force" within the National Association of Secretaries of State ("NASS") in order to "combat threats" and fostering "technical forums for those who are directly responsible for protecting digital election processes and systems." Ex. 29, at 7–8. The states are continuing "to increase protection for their own systems." Ex. 29, at 9. But election systems face unique threats that require special expertise and protective measures, which make them "fundamentally different from any other sector or subsector of critical infrastructure." Ex. 29, at 6.

The Commission's plan to aggregate all state voter roll data into a single database would do nothing to mitigate these threats and, in fact, it would only introduce new vulnerabilities. Indeed, the Georgia state Director of Elections said, in response to the Commission's June 28, 2017, letter that the Commission's instructions were not consistent with state "security protocol." Letter from Chris Harvey, Director of Elections, Georgia Secretary of State's Office, to Kris W. Kobach, Vice Chair, Presidential Advisory Commission on Election Integrity (July 3, 2017), Ex. 20.

II. The Establishment of the Commission

The Presidential Advisory Commission on Election Integrity was established by executive order on May 11, 2017. Exec. Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017), Ex. 1. The Vice President is named as the Chair of the Commission, "which shall be composed [sic] of not more than 15 additional members." *Id.* Additional members are appointed by the President, and the Vice President may select a Vice Chair of the Commission from among the members. *Id.* Vice President Pence has named Kansas Secretary of State Kris Kobach to serve as Vice Chair of the Commission.

The Commission was asked to "*study* the registration and voting processes used in Federal elections." *Id.* (emphasis added). The Commission was further asked to identify "(a) those laws,

18-F-1517//0876

rules, policies, activities, strategies, and practices that enhance the American people's confidence in the integrity of the voting processes used in Federal elections; (b) those laws, rules, policies, activities, strategies, and practices that undermine the American people's confidence in the integrity of the voting processes used in Federal elections; and (c) those vulnerabilities in voting systems and practices used for Federal elections that could lead to improper voter registrations and improper voting, including fraudulent voter registrations and fraudulent voting." *Id.*

There is no authority in the Executive Order to subpoena records, to undertake investigations, or to demand the production of state voter records from state election officials.

III. The Role of the General Services Administration

The Executive Order provides that the GSA "shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis." 82 Fed. Reg. at 22,390, Ex. 1, at 2. The Commission Charter designates the GSA as the "Agency Responsible for Providing Support," and similarly orders that the GSA "shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis." Charter, Presidential Advisory Commission on Election Integrity ¶ 6, First Kobach Decl., Ex. 2.

The GSA routinely conducts and publishes Privacy Impact Assessments when it collects, maintains, and uses personal information on individuals. Gen. Serv. Admin., *Privacy Impact Assessments* (Apr. 13, 2017), Ex. 18. There is no authority in the Executive Order of the Commission Charter for any other entity to provide "administrative services," "facilities," or "equipment" to "carry out [the Commission's] mission."

IV. The Role of Other Government Agencies and Officials

The Commission revealed for the first time in its supplemental brief that the Director of White House Information Technology is now in charge of "repurposing an existing system" within the "White House Information Technology enterprise." Def.'s Supp. Br. 2, ECF No. 24.

18-F-1517//0877

Although the Commission did not provide the name of the current Director of White House Information Technology, EPIC was able to identify that individual as Mr. Charles C. Herndon, and name him as a codefendant in the Second Amended Complaint. Second Am. Compl. ¶ 10, ECF No. 33.

The "information resources and information systems" in the Executive Office of the President, which the Director has primary authority to oversee, include the resources of the U.S. Digital Service, which is housed within the Office of Management and Budget. U.S. Digital Serv., *Report to Congress — December 2016* at 4 (2016), Ex. 36. The U.S. Digital Service is responsible for "improving performance and cost-effectiveness of important government digital services." *Id.* The Director of White House Information Technology, the Executive Committee for Presidential Information Technology, and the U.S. Digital Service are all components within the EOP and thus subject to both the APA and the E-Government Act.

In addition, one of the Commission members, Christy McCormick is also a member of the Election Assistance Commission ("EAC"). Kobach Second Decl. 2, ECF No. 11-1. The EAC is an agency under the APA and is subject to the E-Government Act.

V. The Commission's Demand for State Voter Records

On June 28, 2017, the Commission undertook an unprecedented effort to collect detailed voter records from all fifty states and the District of Columbia. For example, the Commission sent a letter to North Carolina Secretary of State Elaine Marshall. Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), Ex. 3 ("Commission Letter"). In the letter, Kobach asked Marshall to provide to the Commission

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony

18-F-1517//0878

> convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.

Id. at 1–2.

The fact that the Commission demanded State election officials to turn over sensitive personal information that raises many privacy concerns. For example, the improper collection and use of Social Security Numbers ("SSNs") is a major contributor to identity theft in the United States. Soc. Sec. Admin., *Identity Theft and Your Social Security Number* (Feb. 2016).[4] "An estimated 17.6 million Americans—about 7% of U.S. residents age 16 or older—were victims of identity theft in 2014." Erika Harrell, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* at 1 (Sept. 2015).[5] U.S. victims of identity theft lost a collective total of $15.4 billion in the same year. *Id.* at 7.

Collecting and publishing the home addresses of current and former military personnel also poses privacy and security risks. The U.S. Military routinely redacts "names, social security numbers, personal telephone numbers, home addresses and personal email addresses" of military personnel in published documents, "since release would constitute a clearly unwarranted invasion of their personal privacy." U.S. Pacific Fleet, *Report of the Court of Inquiry* (2001);[6] *see also* Def. Logistics Agency, *Defense Logistics Agency Instruction 6303* (2009)[7] (noting that military home addresses are "For Official Use Only" and must be redacted prior to public release of documents); Jason Molinet, *ISIS Hackers Call for Homegrown 'Jihad' Against U.S. Military, Posts Names and Addresses of 100 Service Members*, N.Y. Daily News (Mar. 21, 2015).[8]

---

[4] https://www.ssa.gov/pubs/EN-05-10064.pdf.
[5] https://www.bjs.gov/content/pub/pdf/vit14.pdf.
[6] http://www.cpf.navy.mil/subsite/ehimemaru/legal/GREENEVILLE_FOIA_exemption.pdf.
[7] http://www.dla.mil/Portals/104/Documents/J5StrategicPlansPolicy/PublicIssuances/i6303.pdf.
[8] http://www.nydailynews.com/news/national/isis-hackers-call-jihad-u-s-military-article-1.2157749.

18-F-1517//0879

In the Commission Letter, the Kobach warned that "any documents that are submitted to the full Commission w[ould] also be made available to the public." Commission Letter 2. Kobach later stated that "the Commission intends to de-identify any such data prior to public release of the documents." First Kobach Decl. ¶ 5. However, the Commission has given "no identification or description of the process or technique, no explanation of what the Commission hopes to protect and how they can ensure they have done so, and no description of the reason for publishing anything." Decl. of Cynthia Dwork ¶ 7, Ex. 23. There is an "inherent contradiction" in the Commission's simultaneous statements that there is no privacy interest in the voter data and that the Commission will take steps to protect the privacy of the data.

Kobach stated that he expected a response from the states by July 14, 2017—approximately ten business days after the date of the request—and instructed that the State Secretary could submit her responses "electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange" system. *Id.* Neither the email address nor the file exchange system proposed by the Commission provides a secure mechanism for transferring sensitive personal information. In fact, an attempt to access the File Exchange system linked in the letter leads to a warning screen with a notification that the site is insecure. *See* Second Decl. of Harry R. Lewis, Ex. 17; Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Site (July 3, 2017 12:02 AM), Ex. 6.

Similar letters were sent to election officials in the other 49 states and the District of Columbia. First Kobach Decl. ¶ 4.

VI. Relationship Between the Commission's Request and the Vice Chair's Interstate Voter Registration Crosscheck Program

The Commission's request for state voter records also raises significant privacy concerns because of the Vice Chair's previous attempts to collect and match state voter records, an activity that if undertaken by a federal agency, would trigger numerous requirements under the federal Privacy Act. 5 U.S.C. § 552a *et seq*. Beginning in 2011, the Vice Chair of the Commission, acting as the Secretary of State of Kansas, "made it one of [his] highest priorities to increase the number

18-F-1517//0880

of participating states" in the Interstate Voter Registration Crosscheck Program ("Crosscheck Program"). Sec'y of State, Kansas, *Interstate Crosscheck Program Grows* 2 (2013), Ex. 33. The "Crosscheck Program," which "began as an arrangement between Kansas, Iowa, Nebraska, and Missouri, involves the collection of voter information including 13 data elements—status, date generated, first name, middle name, last name, suffix name, date of birth, voter id number, last 4 digits of SSN, mailing address, county, date of registration, and voting history. Presentation by Kris W. Kobach to the National Ass'n of State Election Dirs., *Interstate Voter Registration Crosscheck Program* 8 (Jan. 26, 2013), Ex. 34. The voter data elements requested by Kobach in the Crosscheck program are nearly identical to the data elements demanded by Kobach in June 28, 2017, letter to the states.

The Vice Chair's attempt to gather voter data from 50 states and the District of Columbia appears to be an attempt to extend the Crosscheck program under federal authority but outside law. One indication of the intent to run Crosscheck from the Commission is that the FTP site for the Crosscheck program is "hosted by Arkansas," Ex. 34, at 11, and Arkansas was the first state to submit voter data to the Commission in response to Kobach's June 28, 2017, demand. TRO Hr'g Tr. 41, July 7, 2017.

Reviews of the Crosscheck system have shown that it generates false positives and can lead to improper removal of voters from the active rolls. A 2016 investigation conducted by Rolling Stone, including a review of Crosscheck lists from Virginia, Georgia, and Washington, showed more than "1 million matches – and Crosscheck's results seemed at best deeply flawed." Greg Palast, *The GOP's Stealth War Against Voters*, Rolling Stone (Aug. 24, 2016), Ex. 35. A grid based on the 2012 Crosscheck data, provided in Kobach's 2013 presentation to the National Association of State Election Directors, shows more than 1 million "potential duplicate voters" in 15 states. Ex. 34, at 10. A database expert who reviewed the data from three states as part of the Rolling Stone investigation said that "he was shocked by Crosscheck's 'childish methodology'" which "spews out little more than a bunch of common names." Ex. 35. Oregon abandoned the

18-F-1517//0881

Crosscheck program after 2014 because, as the secretary of state explained, "the data we received was unreliable." Ex. 35.

VII. Developments Since the Commission Sent Its June 28, 2017, Letter to the States

There have been several significant developments since Kobach sent the June 28th letter demanding that all states transfer personal voter data to the Commission by July 14, 2017. First, in response to EPIC's Emergency Motion, Kobach stated that, "as of July 5, 2017, no Secretary of State had yet provided to the Commission any of the information requested in [his] letter." First Kobach Decl. ¶ 6. Then counsel for Defendants subsequently revealed at the July 7, 2017, hearing that Arkansas had submitted data via the Department of Defense file exchange system. TRO Hr'g Tr. 41, July 7, 2017. Counsel for the Defendants was unable to provide the Court with any details concerning where the voter data would be stored, whether it would be secured, and what government entities would be involved in the collection and storage of the data. Hr'g Tr. 33–36.

Prior to the hearing, EPIC located and submitted to the Court a copy of the Privacy Impact Assessment that the Army had conducted and published for the file exchange system. *See* Ex. 22. According to the Department of Defense PIA, the file exchange system was not authorized to be used to "collect, maintain, use, and/or disseminate" personally identifiable information from "members of the general public." Ex. 22, at 1. After EPIC filed an amended complaint adding the Department of Defense as a codefendant, the Defendants announced in a supplemental brief that the Commission intended to "use alternative means for transmitting the requested data." Def.'s Supp. Br. 1, ECF No. 24. The Defendants stated that "[t]he Commission will not download the data that Arkansas already transmitted" to the file exchange system and that the "data will be deleted from the site." *Id.* The Defendants have not confirmed that the data has, in fact, been deleted.

The Defendants also revealed for the first time in their supplemental brief that the "Director of White House Information Technology is repurposing an existing system" to be used for the collection of personal voter data that the Commission demanded from the states. *Id.* The

18-F-1517//0882

Defendants claimed that "[t]he system is anticipated to be fully functional by 6:00 pm EDT [on July 10, 2017]." *Id*. The Commission did not provide any indication it would complete a Privacy Impact Assessment prior to a subsequent request for data from the states. The Commission did not provide any indication it would publish the Privacy Impact Assessment pursuant to the FACA. The Commission did not explain how it could delegate White House personnel to manage the facilities for the Commission when both the Executive Order and the Commission Charter make clear that the General Services Administration ("GSA") is the "agency responsible" for this function.

VIII. The States Have Opposed the Commission's Request

As of July 6, 2017, only one state in the country had complied with the Commission's request. The vast majority of states have refused to turn over the voter data the Commission is seeking. *Forty-four states and DC have refused to give certain voter information to Trump commission,* CNN (July 5, 2017).[9] California Secretary of State Alex Padilla stated on June 29, 2017, that "[t]he President's commission has requested the personal data and the voting history of every American voter–including Californians. As Secretary of State, it is my duty to ensure the integrity of our elections and to protect the voting rights and privacy of our state's voters." Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017).[10] Nebraska Secretary of State John Gale stated on July 6, 2017 that "I also have a concern about data privacy. I have no clear assurances about the security that this national database will receive. In light of the domestic and foreign attacks in 2016 on state voter registration databases, the commission will need to assure my office

[9] http://www.cnn.com/2017/07/03/politics/kris-kobach-letter-voter-fraud-commission-information/index.html.

[10] http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/.

18-F-1517//0883

of a high level of security." Press Release, Sec. Gale Issues Statement on Request for NE Voter Record Information (July 6, 2017).[11] Arizona Secretary of State Michele Reagan said:

> I share the concerns of many Arizona citizens that the Commission's request implicates serious privacy concerns. [...] Since there is nothing in Executive Order 13799 (nor federal law) that gives the Commission authority to unilaterally acquire and disseminate such sensitive information, the Arizona Secretary of State's Office is not in a position to fulfill your request. [...]
> Centralizing sensitive voter registration information from every U.S. state is a potential target for nefarious actors who may be intent on further undermining our electoral process. [...] Without any explanation how Arizona's voter information would be safeguarded or what security protocols the Commission has put in place, I cannot in good conscience release Arizonans' sensitive voter data for this hastily organized experiment.

Letter from Michele Reagan, Arizona Sec. of State, to Kris Kobach (July 3, 2017).

IX. Defendants' Failure to Conduct a Privacy Impact Assessment

Under the E-Government Act of 2002, any agency "initiating a new collection of information that (I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual" is required to complete a privacy impact assessment ("PIA") before initiating such collection. Pub. L. 107–347, 116 Stat. 2899, Title II § 208 (codified as amended at 44 U.S.C. § 3501 note). The agency must:

> (i) [C]onduct a privacy impact assessment; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

Id. The Privacy Impact Assessment would require the agency to state:

> (I) what information is to be collected;
> (II) why the information is being collected;
> (III) the intended use of the agency of the information;
> (IV) with whom the information will be shared;

[11] http://www.sos.ne.gov/admin/press_releases/pdf-2017/nr-20170707.pdf.

18-F-1517//0884

> (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
> (VI) how the information will be secured; and
> (VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the ''Privacy Act'').

Id. § 208 (b)(2)(B)(ii).

That assessment is particularly important here because the E-Government Act also requires the agency to "ensure that":

> a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and

Id. § 208 (b)(2)(B)(ii).

It is certainly conceivable that a proper Privacy Impact Assessment would have led to the conclusion that the Commission simply could not request and collect state voter record information. Moreover, under the Federal Advisory Committee Act, the Defendants would have been required to make available the Privacy Impact Assessment to the Public. 5 U.S.C. app. 2 § 10(b).

But none of the Defendants have conducted a privacy impact assessment for the Commission's proposed collection of state voter data or the Director of White House Information Technology's development of a system to collect the data. None of the Defendants have ensured review of a PIA by any Chief Information Officer or equivalent official. The Commission has not made any PIA available to the public. Complaint ¶¶ 32–34.

STANDARD OF REVIEW

In order to obtain a temporary restraining order or preliminary injunction, a plaintiff must show that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm in the absence of preliminary relief, (3) that the balance of the equities tips in their favor, and (4) that an injunction is in the public interest. *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011) (quoting *Winter v. NRDC*, 555 U.S. 7, 20 (2008)). This Court has held that plaintiff's are entitled

18-F-1517//0885

to preliminary injunctive relief where, as here, they "have shown a clear likelihood of success on the merits and have satisfied the other requirements for a preliminary injunction." *Dimondstein v. American Postal Workers Union*, 964 F.Supp.2d 37, 41 (D.D.C. 2013). The D.C. Circuit has adopted a "sliding scale" approach when evaluating these injunction factors. *Sherley*, 644 F.3d at 392. Thus if the "movant makes an unusually strong showing on one of the factors, then it does not necessarily have to make a strong showing on another factor." *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1291–92 (D.C. Cir. 2009). *But see League of Women Voters of U.S. v. Newby*, 838 F.3d 1, 7 (D.C. Cir. 2016) (noting that the court has "not yet decided" whether the sliding scale approach applies post-*Winter*). Preliminary injunctive relief is especially appropriate where, as here, it is necessary "to preserve the status quo and to prevent irreparable harm." *CAIR v. Gaubatz*, 667 F. Supp. 2d 67, 79 (D.D.C. 2010).

ARGUMENT

This case presents the type of extraordinary circumstance that justifies preliminary injunctive relief. Absent a prohibition from this Court, the Commission will begin collecting and aggregating the sensitive, personal information of voters across the country without establishing any procedures to protect voter privacy or the security and integrity of the state voter data. There is already evidence that the Commission has placed and will place voter data at risk.

First and foremost, this proposed collection violates a core provision of the E-Government Act of 2002, which requires that agencies establish sufficient protections *prior* to initiating any new collection of personal information using information technology. The Commission's actions also violate voters' Fifth Amendment right to informational privacy and, through their implementation, violate the Administrative Procedure Act (APA). Second, this collection and aggregation of sensitive personal information, as well as the exposure of this voter data through insecure systems, will cause irreparable harm to EPIC and its members. The Commission has demanded that states provide confidential voter information, the improper transfer of which is a *per se* harm. In addition, the collection and aggregation of this sensitive data will exacerbate the

18-F-1517//0886

already acute risks to voter data, and create a new target for malicious hackers. If this data were to be hacked, there would be no way to control its spread. Third, the balance of the equities favors relief because the Commission will suffer no hardship if the collection is enjoined pending resolution of the case; indeed the Commission has already conceded this point by halting collection pending resolution of EPIC's motion. Fourth, granting the injunction would be in the public interest. The Commission's mandate is to "study" election integrity. There is nothing in the Executive Order or the Commission's Charter that provides authority to gather hundreds of millions of voter records from the states or to create a secret database stored in the White House. The Commission's actions, apart from its stated role, far exceed a solely "advisory" function. As evidenced by the response of state officials of both political parties to the Commission's June 28, 2017 letter, the Commission's request has in fact undermined "the American's people's confidence in the integrity of the voting processes used in federal elections." Ex. 1. By the terms of the Commission's purpose and the actions undertaken by the Commission, the order EPIC seeks should be granted.

I. EPIC is likely to succeed on the merits of its claims.

A. Defendants Proposed Collection of State Voter Data Violates the E-Government Act and the APA

The Defendants have made no attempt to comply with the Privacy Impact Assessment requirements of Section 208 of the E-Government Act of 2002, Pub. L. 107-347, 115 Stat. 2899, Title II § 208 (codified at 44 U.S.C. § 3501 note), which are clearly applicable to the collection of sensitive, personal information from state voter databases. The Defendants' actions therefore violate the Administrative Procedures Act ("APA"), 5 U.S.C. § 706(2)(A). EPIC is likely to succeed on its statutory claims.

As the Department of Justice has explained, "Privacy Impact Assessments ("PIAs") are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing

18-F-1517//0887

information technology that manages information in identifiable form." Office of Privacy & Civil Liberties, U.S. Dep't of Justice, *E-Government Act of 2002* (June 18, 2014).[12] A Privacy Impact Assessment is "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." Joshua B. Bolten, Director, Office of Mgmt. & Budget, Executive Office of the President, M-03-22, Memorandum for Heads of Executive Departments and Agencies, Attachment A (Sept. 26, 2003) [hereinafter Bolten Memo], Ex. 5.

The E-Government Act requires that an agency "shall take actions described under subparagraph (B)" of Section 208 "before . . . initiating a new collection of information that—(I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government." E-Government Act § 208(b)(1)(A)(ii). The actions described in subparagraph (B), which the Commission must take *before* collecting this information, include "(i) conduct[ing] a privacy assessment; (ii) ensur[ing] the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), mak[ing] the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." E-Government Act § 208(b)(1)(B).

The Commission has already "initiated a new collection" of personal information, but it has not complied with any of these requirements. The APA prohibits federal agencies from taking

[12] https://www.justice.gov/opcl/e-government-act-2002.

18-F-1517//0888

any action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2). The Commission's actions are "not in accordance with law." The APA authorizes this Court to "compel agency action unlawfully withheld." 5 U.S.C. § 706(1). Such a claim may proceed "where a plaintiff asserts that an agency failed to take a *discrete* agency action that it is *required to take.*" *Norton v. S. Utah Wildlife Alliance*, 542 U.S. 55, 64 (2004). An agency's failure to comply with the PIA requirements of the E-Government Act is reviewable under both provisions of APA § 706. *Fanin v. Dep't of Veteran Affairs*, 572 F.3d 868, 875 (11th Cir. 2009).

The E-Government Act defines "information technology" as "any equipment or interconnected system . . . used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly . . . ." 40 U.S.C. § 11101(6); *see* E-Government Act § 201 (applying definitions from 44 U.S.C. §§ 3502, 3601); 44 US.C. § 3502(9) (applying the definition of 40 U.S.C. § 11101(6)). Courts have found that a "minor change" to "a system or collection" that does not "create new privacy risks," such as the purchasing of a new external hard drive, would not require a PIA. *Perkins v. Dep't of Veteran Affairs*, No. 07-310, at *19 (N.D. Ala. Apr. 21, 2010) (quoting Bolten Memo § II.B.3.f). However, an agency is obligated to conduct a PIA before initiating a new collection of data that will be "collected, maintained, or disseminated using information technology" whenever that data "includes any information in identifiable form permitting the physical or online contacting of a specific individual" and so long as the questions have been posed to 10 or more persons. E-Government Act § 208(b)(1)(A)(ii). The term "identifiable form" means "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." E-Government Act § 208(d).

There is no question that the PIA requirement applies in this case. The Commission's decision to initiate collection of comprehensive voter data by requesting personal information

18-F-1517//0889

from Secretaries of State of all 50 states and the District of Columbia, including sensitive, personal information about hundreds of millions of voters, triggers the obligations of § 208(b)(1)(A)(ii). The letter sent by Commission Vice Chair Kobach requests that the Secretary of State provide "voter roll data" including "the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas information." Commission Letter 1–2. The states are instructed to submit their "responses *electronically* to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE")," a government website used to transfer files. *Id.* (emphasis added).[13] This sensitive voter roll data is precisely the type of "personal information" in "identifiable form" that the PIA provision was intended to protect, and the transfer of large data files via email or otherwise clearly involves the use of information technology.

As the court explained in *Perkins*, PIAs are necessary to address "(1) what information is collected and why, (2) the agency's intended use of the information, (3) with whom the information would be shared, (4) what opportunities the [individuals] would have to decline to provide information or to decline to share the information, (5) how the information would be secured, and (6) whether a system of records is being created." *Perkins v. Dep't of Veteran Affairs*, No. 07-310, at *19 (N.D. Ala. Apr. 21, 2010). *See* E-Government Act § 208(b)(2)(B); Bolten Memo § II.C.1.a. These types of inquiries are "certainly appropriate and required" when an agency "initially created" a new database system and "began collecting data." *Perkins*, No. 07-310, at *19–20.

[13] The government file exchange website is not actually "safe." In fact, any user who follows the link provided in the Commission Letter will see a warning that the site is insecure. Ex 6.

18-F-1517//0890

B. The Executive Office of the President, the Commission, and the Director of White House Information Technology are Agencies Subject to the Administrative Procedure Act and the E-Government Act

The Commission has claimed that it is not subject to either the APA or the E-Government Act, but these arguments are contrary to the plain text of the statutes and unsupported by case law or legislative history. *See* Mem. Op. 9-13. The Commission fits squarely within the broad statutory definition of an "agency" in both the APA and the E-Government Act. *See* 5 U.S.C. § 551(1); 44 U.S.C. § 3502. The Commission does not dispute that if the APA and E-Government Act apply, the failure to conduct a PIA violates federal law. EPIC has therefore established a clear likelihood of success on the merits, which justifies entry of a TRO or injunction.

1. The EOP and its subcomponents are agencies under the APA.

The Executive Office of the President ("EOP") and its constituent offices are "agenc[ies]" within the meaning of the Administrative Procedure Act ("APA"). Under the APA, "each authority of the Government of the United States" is an agency "whether or not it is within or subject to review by another agency[.]" 5 U.S.C. § 551(1). "[T]he APA inquiry into agency status is . . . focused on the functions of the entity, and flexible enough to encompass the 'myriad organizational arrangements for getting the business of government done.'" *Meyer v. Bush*, 981 F.2d 1288, 1304 (D.C. Cir. 1993) (quoting *Washington Research Proj., Inc. v. HEW,* 504 F.2d 238, 246 (D.C. Cir. 1974)). "The legislative history of the APA indicates that Congress wanted to avoid a formalistic definition of 'agency' that might exclude any authority within the executive branch that should appropriately be subject to the requirements of the APA." *Armstrong v. Bush*, 924 F.2d 282, 291 (D.C. Cir. 1991).

The EOP is emphatically an "authority of the government" for "getting the business of government done." 5 U.S.C. § 551(1); *Meyer*, 981 F.2d at 1304; *see Executive Office of the President*, The White House (2017)[14] ("The EOP has responsibility for tasks ranging from communicating the President's message to the American people to promoting our trade interests

[14] https://www.whitehouse.gov/administration/eop.

18-F-1517//0891

abroad."). The EOP consists of a dozen or more major subcomponents that oversee and carry out vital government functions, including the National Security Council (charged with "integrating all aspects of national security policy as it affects the United States"); the Office of Management and Budget (charged with "supervis[ing] and control[ling] the administration of the budget"); and the Office of the United States Trade Representative (an office headed by a "Cabinet-level official" who "acts as the chief representative of the United States in all General Agreement on Tariffs and Trade activities"). *The Executive Office of the President*, The United States Government Manual.[15] The EOP is clearly a "center of gravity in the exercise of administrative power" wielding "substantial independent authority," and thus an "agency" under § 551(1). *Dong v. Smithsonian Inst.*, 125 F.3d 877, 881–882 (D.C. Cir. 1997); *cf. Pub. Citizen v. Carlin*, 2 F. Supp. 2d 1, 9 (D.D.C. 1997), *rev'd on other grounds*, 184 F.3d 900 (D.C. Cir. 1999) ("The EOP's status as an agency is also evidenced by the authority it possesses to impose requirements on all of the EOP components in certain matters.").

The EOP subcomponents named in EPIC's suit are likewise "agenc[ies]" under the APA. The Commission, which includes both the Vice President and a principal member of the Election Assistance Commission, is authorized to "study[] registration and voting processes" and to identify "which laws, rules, policies, activities, strategies, and practices that enhance or undermine Americans' confidence in the integrity of the federal election process." First Kobach Declaration 1, 3, ECF No. 8-1; Second Kobach Declaration 1, ECF 11-1. In practice, the Commission has gone well beyond its mandate to engage in substantive conduct that "affect[s] the rights" of individuals. *Dong*, 125 F.3d at 881 (quoting James O. Freedman, *Administrative Procedure and the Control of Foreign Direct Investment*, 119 U. Pa. L. Rev. 1, 9 (1970)).

Two weeks ago, the Commission undertook to assemble a database of personal voter information that directly implicates the privacy rights of least 157 million registered voters across

[15] https://www.usgovernmentmanual.gov/(S(zqmgxvxx0zutkos5uua3cyc4))/Agency.aspx?EntityId=p0fnvDxExmY=&ParentEId=+klubNxgV0o=&EType=jY3M4CTKVHY (last visited July 12, 2017).

18-F-1517//0892

50 states and the District of Columbia. Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), Ex. 3; U.S. Census Bureau, Voting and Registration in the Election of November 2016 at tbl. 4a (May 2017).[16] This sweeping depository of personal data would put the Internal Revenue Service—with its yearly haul of just 149 million individual returns—to shame. Internal Revenue Serv., *SOI Tax Stats - Tax Stats at a Glance* (2016).[17] "[A]ny authority within the executive branch" engaged in such far-reaching conduct is "appropriately subject to the requirements of the APA." *Armstrong*, 924 F.2d at 291; *cf. Meyer*, 981 F.2d at 1298 (Wald, J., dissenting) ("Congress contemplated that 'agency' would encompass entities, like the Task Force, which are created solely by executive order.").

Defendant Charles C. Herndon, Director of White House Information Technology ("the Director"), also oversees an "authority of the Government" that is a "center of gravity in the exercise of administrative power."[18] 5 U.S.C. § 551(1); *Dong*, 125 F.3d at 881; Def. Resp. to Pl. Mot. to Amend, ECF No. 32. The Director and his staff enjoy "primary authority to establish and coordinate the necessary policies and procedures for operating and maintaining the information resources and information systems provided to the President, Vice President, and EOP." Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology § 1, 2015 Daily Comp. Pres. Doc. 185 (Mar. 19, 2015), Ex. 25. This authority includes:

> [providing] policy coordination and guidance for, and periodically review[ing], all activities relating to the information resources and information systems provided to the President, Vice President, and EOP by the Community, including expenditures for, and procurement of, information resources and information systems by the Community. Such activities shall be subject to the Director's coordination, guidance, and review in order to ensure consistency with the Director's strategy and to strengthen the quality of the Community's decisions through integrated analysis, planning, budgeting, and evaluating process.

---

[16] https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-580.html.
[17] https://www.irs.gov/uac/soi-tax-stats-tax-stats-at-a-glance.
[18] The White House Office ("WHO"), of which the Director is a part, also qualifies as an agency. The WHO is charged with the authority to "facilitate[] and maintain[] communication with the Congress, the heads of executive agencies, the press and other information media, and the general public." *The Executive Office of the President*, *supra*.

18-F-1517//0893

Id. § 2(c). The Director may also "advise and confer with appropriate executive departments and agencies, individuals, and other entities as necessary to perform the Director's duties . . . ." *Id.* § 2(d). These grants of authority and responsibility are quintessential features of an APA "agency."

Moreover, the actions of the EOP and its component offices have long been subject to APA review. *Pub. Citizen v. U.S. Trade Representative*, 5 F.3d 549, 551 (D.C. Cir. 1993) ("Public Citizen must rest its claim for judicial review [of U.S. Trade Representative's action] on the Administrative Procedure Act."); *Armstrong v. Bush*, 924 F.2d 282, 291 (D.C. Cir. 1991) ("[W]e find that there is APA review of the [National Security Council]'s recordkeeping guidelines and instructions . . . ."); *Armstrong v. Exec. Office of the President*, 810 F. Supp. 335, 338 (D.D.C. 1993) (citing *Armstrong*, 924 F.2d at 291–293) ("The Court of Appeals . . . approved of this Court's holding that the APA provides for limited review of the adequacy of the NSC's and EOP's recordkeeping guidelines and instructions pursuant to the FRA."); *Citizens for Responsibility & Ethics in Washington (CREW) v. Exec. Office of President*, 587 F. Supp. 2d 48, 57–58, 63 (D.D.C. 2008) (holding that the EOP was properly named as a defendant in an APA and Federal Records Act suit); *Pub. Citizen Health Research Grp. v. Comm'r, Food & Drug Admin.*, 724 F. Supp. 1013, 1023 (D.D.C. 1989) (reviewing OMB inaction under the APA). Indeed, the only part of the EOP that courts have categorically excluded from APA review is the President himself—an official who is not named in this suit. *Franklin v. Massachusetts*, 505 U.S. 788, 800–01 (1992).

The legislative history of the APA further confirms that the EOP and its subcomponents are "agenc[ies]" under the statute. The APA empowers a court to review the actions of a government authority unless there is a "showing of clear and convincing evidence of a legislative intent to restrict access to judicial review." *Citizens to Pres. Overton Park, Inc. v. Volpe*, 401 U.S. 402, 410 (1971) (quotation marks omitted), *abrogated on other grounds by Califano v. Sanders*, 430 U.S. 99 (1977). Yet the legislative history of the APA reveals no Congressional desire at all to shield the actions of the EOP and its subcomponents from judicial review. Quite the opposite.

18-F-1517//0894

As Congress has explained, the term "agency" under the APA is "defined substantially" as it was in the Federal Reports Act of 1942, Pub. L. No. 77-831, § 7(a), 56 Stat. 1078, 1079–80 (1942) (current version at 44 U.S.C. § 3502), and the Federal Register Act, Pub. L. No. 74-220, § 4, 49 Stat. 500, 501 (1935) (current version at 44 U.S.C. § 1501). Administrative Procedure Act, Legislative History, S. Doc. No. 248, at 12–13 (1946); *see also In re Fid. Mortg. Inv'rs*, 690 F.2d 35, 38 (2d Cir. 1982). The Federal Reports Act defined "agency" in exceptionally broad terms: "any executive department, commission, independent establishment, corporation owned or controlled by the United States, board, bureau, division, service, office, authority, or administration in the executive branch of the Government . . . ." § 7(a), 56 Stat. at 1079–80 (emphases added). The Federal Register Act's definition of "agency" even encompassed "the President of the United States," as well as "any executive department, independent board, establishment, bureau, agency, institution, commission, or separate office of the administrative branch of the Government of the United States[.]" § 4, 49 Stat. at 501 (emphases added). Because Congress has made clear that the meaning of "agency" under the APA is "substantially" coextensive with these earlier enumerated definitions, it follows that the EOP, the Commission, and the Director's office are all agencies themselves.

Notably, even if the Defendant subcomponents of EOP did not qualify as agencies themselves, the EOP would be answerable for their actions under the APA because it is a parent agency. *N. Slope Borough v. Andrus*, 642 F.2d 589, 605 (D.C. Cir. 1980) (ascribing actions by National Oceanic and Atmospheric Administration to parent agency Secretary of the Interior in an APA case); *Nat'l Wildlife Fed'n v. Burford*, 835 F.2d 305, 308 (D.C. Cir. 1987) (ascribing actions by Bureau of Land Management to parent agency Department of the Interior in an APA case); *Beverly Health & Rehab. Servs., Inc. v. Thompson*, 223 F. Supp. 2d 73, 75 (D.D.C. 2002); (ascribing actions by Health Care Financing Administration to parent agency Department of Health and Human Services in an APA case); *Indian River Cty. v. Rogoff*, 201 F. Supp. 3d 1, 19 (D.D.C. 2016) (ascribing actions by Federal Railroad Administration to parent agency Department of Transportation in an APA case).

18-F-1517//0895

And even if the Commission were solely an advisory committee—which, to be clear, it is not—the EOP would remain its parent agency for the purposes of both the APA and the FACA. *See* TRO Hr'g Tr. 29:14–17 (statement of Elizabeth J. Shapiro that Commission is located in "the Office of the Vice President, since the vice president is chair of the Committee"); *The Executive Office of the President*, *supra* (identifying the Office of the Vice President as a subcomponent of the EOP). The EOP would thus be subject to APA review for the Commission's unlawful nondisclosure of records under FACA. *Ctr. for Biological Diversity v. Tidwell*, No. CV 15-2176 (CKK), 2017 WL 943902, at *9 (D.D.C. Mar. 9, 2017) ("[T]he Court finds that Plaintiff has pleaded a viable claim under the APA for a violation of section 10(b), as the Complaint plausibly alleges that the [committee] was a FACA advisory committee, and that the [parent agency] failed to disclose the materials required by section 10(b).").

2. The Soucie 'sole function' exception does not apply to the APA's definition of 'agency.'

The "sole function" exception, which excuses a small circle of presidential advisors from the FOIA's "agency" disclosure requirements, simply does not apply to the APA's definition of "agency." This is apparent from the FOIA-specific origins of the "sole function" exception and the legislative history of the 1974 FOIA amendments.

The "sole function" exception derives from *Soucie v. David*, 448 F.2d 1067 (D.C. Cir. 1971), a case that highlighted potential conflicts between FOIA's presumption of openness and the President's power to assert executive privilege. In *Soucie*, the D.C. Circuit held that a subcomponent of the EOP, the Office of Science and Technology ("OST"), was an agency "subject to the public information provisions of the APA, i.e., the Freedom of Information Act."[19] *Id.* at 1073, 1075. But the court—wary of how an assertion of executive privilege might play out "in the context of a congressional command to disclose information"—added a narrow caveat in

[19] In the early years of the FOIA, the statute was sometimes characterized as a subpart of the APA. *E.g., Nat'l Parks & Conservation Ass'n v. Kleppe*, 547 F.2d 673, 678 n.16 (D.C. Cir. 1976) (citing Statement by the President Upon Signing Bill Revising Public Information Provisions of the Administrative Procedure Act, Weekly Comp. Pres. Doc. 895 (July 4, 1966)).

18-F-1517//0896

dicta: "If the OST's sole function were to advise and assist the President, that might be taken as an indication that the OST is part of the President's staff and not a separate agency." *Id.* at 1071 n.9, 1075 (emphasis added).

Whatever the force of this statement in a FOIA context, it certainly does not preclude APA review where, as here, the EOP is engaged in substantive conduct directly "affecting the rights and obligations of individuals. . . ." *Dong*, 125 F.3d at 881. Rather, the *Soucie* court was concerned about the EOP's nondisclosure of records under FOIA and the "[s]erious constitutional questions [that] would be presented by a claim of executive privilege as a defense to a suit under the Freedom of Information Act." *Soucie*, 448 F.2d at 1071. In other words: *Soucie* addressed the public availability of EOP records and the President's qualified privilege to withhold them, whereas APA review addresses the legality of substantive actions that the EOP takes. The two are distinct.

Congress sharpened this point when it passed the 1974 FOIA amendments, formally distinguishing the FOIA's definition of "agency" from that of the APA. *Compare* 5 U.S.C. § 551(a), *with* 5 U.S.C. § 552(f)(1). Though Congress broadened the textual definition of "agency" under the FOIA in several ways—e.g., making it explicit that the "Executive Office of the President" is subject to the statute—Congress also adopted the *Soucie* court's narrowing construction:

> With respect to the meaning of the term "Executive Office of the President" the conferees intend the result reached in *Soucie v. David* . . . . The term is not to be interpreted as including the President's immediate personal staff or units in the Executive Office whose sole function is to advise and assist the President.

H.R. Rep. No. 93-1380, at 232 (1974) (Conf. Rep.); *see also Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 156 (1980) (interpreting the House report to mean that the words "Executive Office" in the FOIA did "not include the Office of the President"). But in amending the FOIA, Congress left the definition of "agency" under the APA entirely untouched. It thus remains as broad as it ever was.

18-F-1517//0897

Courts have repeatedly declined to carve out a "sole function" exception in the APA's definition of "agency" when reviewing the conduct of EOP units. *Pub. Citizen*, 5 F.3d at 551 (applying APA to U.S. Trade Representative ("USTR") without invoking "sole function" test); *Armstrong*, 924 F.2d at 291 (applying APA to NSC without invoking "sole function" test); *CREW v. EOP*, 587 F. Supp. 2d at 57–58, 63 (applying APA to EOP without invoking "sole function" test); *Pub. Citizen Health Research Grp. v. Comm'r, Food & Drug Admin.*, 724 F. Supp. 1013, 1023 (D.D.C. 1989) (applying APA to OMB without invoking "sole function" test).

In *Alexander v. FBI*, 971 F. Supp. 603 (D.D.C. 1997), the court explained that statutes which "provide citizens with better access to government records" and statutes that "provide certain safeguards for an individual against an invasion of personal privacy" serve "very different purposes." *Id.* at 606. Exceptions that would apply to the definition of "agency" in the former case would thus not apply in the latter case:

> When passing FOIA, Congress was addressing the need for individuals to have access to government information. When passing the Privacy Act, Congress was addressing the need for individuals to have protection for their privacy concerns. In interpreting the word "agency" to exclude, under FOIA, the immediate staff of the President, the courts recognize, as Congress did, that the access provided by FOIA must be limited. However . . . there is no evidence that the privacy protections provided by Congress in the Privacy Act must also be necessarily limited. . . . Thus there is no need to ignore the plain language of the statute and limit the word "agency" as has been done under FOIA . . . .

Id.

This Court's holding in *Sculimbrene v. Reno*, 158 F. Supp. 2d 26 (D.D.C. 2001), is not to the contrary. First, *Sculimbrene* concerned a plaintiff "seeking access, under the Privacy Act, to records pertaining to himself"—effectively a FOIA request styled as a Privacy Act request. *Sculimbrene*, 158 F. Supp. 2d at 28. *Sculimbrene* did not concern substantive conduct that "inva[ded] personal privacy," such as the "improper maintenance of [private] files" at issue in *Alexander* or the unlawful collection of personal voter data at issue here. *Alexander*, 971 F. Supp. at 605. These "very different" circumstances warranted different interpretations of the term "agency." *Id.* at 606. Second, unlike the APA, the Privacy Act relies on precisely the same

18-F-1517//0898

statutory provision as the FOIA to define "agency." 5 U.S.C. § 552a(a)(1) (citing § 552(e)). By contrast, because the APA's definition of "agency" does not reference the FOIA's definition, the APA cannot be said to have incorporated any of FOIA's implicit limitations on that term.

If Congress intended for the APA and FOIA definitions of "agency" to be coextensive, it has had ample opportunity to amend the APA since the 1974 FOIA amendments were enacted. It has not done so. There is no basis in statute, legislative history, or case law to apply the "sole function" exception to the APA's definition of "agency."

3. Even if the 'sole function' exception applied, the EOP and its subcomponents would be agencies under the APA.

The EOP, the Commission, and the Director's office do far more than just "advise and assist the President." Soucie, 448 F.2d at 1075. Thus even if the "sole function" exception applied to the APA, these entities would still be agencies.

The EOP, as noted, carries out a wide array of functions that extend well beyond the immediate needs of the President. *See supra* Part I.B.1. The EOP consists of numerous subcomponents that oversee and carry out vital government functions, many of which—including the NSC, the OMB, and the USTR—have been deemed agencies under the APA in their own right. *See id.* Moreover, the EOP is expressly named as an agency by the FOIA definition from which the "sole function" exception arises. 5 U.S.C. § 552(e). It cannot be seriously contended that the EOP eludes the APA's definition of "agency."

The same is true of the Director's office. As noted, the Director and his staff enjoy "primary authority to establish and coordinate the necessary policies and procedures for operating and maintaining the information resources and information systems provided to the President, Vice President, and EOP." Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology § 1, 2015 Daily Comp. Pres. Doc. 185 (Mar. 19, 2015), Ex. 25. An entity that has primary authority to set policy and procedures for an agency is doing far more than just assisting the President. The Director's authority even extends beyond the EOP. The Director is required to "provide policy

18-F-1517//0899

coordination and guidance for, and periodically review, all activities relating to the information resources and information systems provided to" both the EOP and the Presidential Information Technology Community ("the Community"), including "expenditures for, and procurement of, information resources and information systems by the Community." *Id.* § 2(c). The Community, in turn, consists of multiple high-level officials: "the Assistant to the President for Management and Administration; the Executive Secretary of the National Security Council; the Director of the Office of Administration; the Director of the United States Secret Service; and the Director of the White House Military Office." *Id.* Notably, the Director of the Secret Service is a Department of Homeland Security official. *Overview*, United States Secret Service.[20] Given the broad, interagency reach of the Director's oversight authority, the "sole function" exception is likewise inapplicable to his office.

Finally, the Commission's functions also extend well beyond "advis[ing] and assist[ing]" the President. Here, as in *Energy Research Foundation v. Def. Nuclear Facilities Safety Bd.*, the Commission satisfies the definition of "agency" because it (1) investigates, (2) evaluates, and (3) makes recommendations. 917 F.2d 581, 585 (D.C. Cir. 1990) (citing *Soucie*, 448 F.2d at 1075) ("The Board of course performs precisely these functions. It investigates, evaluates and recommends[.]"); *see* Kobach Decl. 1, 3 (Commission is charged with "studying registration and voting processes"); Kobach Decl. 1 (Commission's report is to identify "which laws, rules, policies, activities, strategies, and practices that enhance or undermine Americans' confidence in the integrity of the federal election process"). Of course the Commission does a great deal more than that, too. It has announced plans to collect, store, and publish the personal data of every registered voter in the country, thereby implicating every voter's individual privacy rights. Kobach Letter 1–2, Ex. 3. The Commission cannot credibly characterize this behavior as incidental to its advisory role: it is acting with the force and effect of an agency. "the record evidence regarding [the Commission]'s actual functions" proves it to be so. *Citizens for*

[20] https://www.secretservice.gov/about/overview/ (last visited June 13, 2017).

18-F-1517//0900

Responsibility & Ethics in Washington (CREW) v. Office of Admin., 559 F. Supp. 2d 9, 26 (D.D.C. 2008), *aff'd*, 566 F.3d 219.

Thus the "sole function" exception, even if applicable to the APA, poses no bar to judicial review of Defendants' actions.

4. The EOP and its subcomponents are 'agencies' under the E-Government Act.

Because the Commission is an "agency" under the APA, it necessarily meets the definition under the E-Government Act as well. 44 U.S.C. § 3502(1). As the Commission itself concedes, the definition of "agency" used in the FOIA is textually broader than that of the APA, Def. Opp'n 10, and the definition of "agency" in the E-Government Act is effectively the same as that of the FOIA. § 3502(1); Def. Opp'n 11. Thus, the E-Government Act's PIA requirement applies with full force to the Commission, just as it would to any other similar Commission. For example, prior to collecting personal data by the Commission on Presidential Scholars ("a group of eminent private citizens appointed by the President to select and honor the Presidential Scholars"), a Privacy Impact Assessment was conducted and Privacy Act notices were issued. U.S. Dep't of Education, U.S. Presidential Scholars Privacy Policy and Impact Assessment (2017).[21]

The FOIA "sole function" exception is also inapplicable here. Although the textual definition of "agency" is essentially the same in the FOIA and the E-Government Act, neither Congress nor any court has said that parts of the EOP should be excused from the plain terms of the E-Government Act. That stands in marked contrast to the FOIA, where Congress and the Supreme Court have accorded a special contextual meaning to the otherwise unambiguous phrase "including the Executive Office of the President." *See supra* Part I.B.2; *Energy Research Found.*, 917 F.2d at 583 ("It is of course possible that identical phrases may carry different meanings in different statutes."). Absent any binding authority to the contrary, the plain text of the E-Government Act controls in this case. *Honeycutt v. United States*, 137 S. Ct. 1626, 1635 n.2

[21] https://www2.ed.gov/programs/psp/applications/privacy.pdf.

18-F-1517//0901

(2017) (emphasizing that courts "cannot construe a statute in a way that negates its plain text"). That text leaves no doubt: the Executive Office of the President, without exception, is subject to the E-Government Act. § 3502(1).

5. The General Services Administration, which is unquestionably an agency under the APA, is obligated to provide the data storage used by the Commission.

None of the above analysis would be necessary if the General Services Administration ("GSA") had provided equipment and facilities for the Commission's proposed storage of personal voter data, just as the GSA was required to do. The President's Executive Order and the Commission's Charter clearly establish that the GSA—not the White House—"shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission . . . ." Exec. Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017), Ex. 1. The GSA is undeniably an agency whose actions are subject to judicial review. *AT&T Info. Sys., Inc. v. GSA*, 810 F.2d 1233 (D.C. Cir. 1987) (applying both the APA and the FOIA to the GSA). To the extent that the Commission might evade the E-Government Act's PIA requirement by using non-GSA facilities to collect voter data, EPIC would face certain informational injury due to the non-disclosure of a PIA. The Court must hold such action unlawful and restrain it.

C. The publication of voters' personal information violates the constitutional right to informational privacy

The Supreme Court has long recognized that individuals have a constitutionally protected interest in "avoiding disclosure of personal matters." *Whalen v. Roe*, 429 U.S. 589, 599 (1977); *accord Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 457 (1977). The constitutionality of a "government action that encroaches upon the privacy rights of an individual is determined by balancing the nature and extent of the intrusion against the government's interest in obtaining the information it seeks." *United States v. District of Columbia*, 44 F. Supp. 2d 53 (D.D.C. 1999); *see also Senior Execs. Ass'n v. United States*, 891 F. Supp. 2d 745, 750–51 (D. Md. 2012) (granting a motion for a preliminary injunction to prohibit disclosure of financial information from executive

18-F-1517//0902

branch and military officials under the STOCK Act). The "individual interest in protecting the privacy of information sought by the government" is more important when that information is to be "disseminated publicly." *Am. Fed'n of Gov't Emps., AFL-CIO v. HUD*, 118 F.3d 786, 793 (D.C. Cir. 1997) [hereinafter *AFGE v. HUD*] (assuming without concluding that the right exists).

In *NASA v. Nelson*, Justice Alito, writing for the Court, said:

> As was our approach in *Whalen*, we will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance. 429 U.S., at 599, 605. We hold, however, that, whatever the scope of this interest, it does not prevent the Government from asking reasonable questions of the sort included on SF-85 and Form 42 in an employment background investigation that is subject to the Privacy Act's safeguards against public disclosure.

NASA v. Nelson, 562 U.S. 134, 147–48 (2011).

The actual holding in *Nelson* is significant in this matter for several reasons. First, the Court in *NASA v. Nelson* observed that in *Whalen v. Roe,* "the Court pointed out that the New York statute contained 'security provisions' that protected against "[p]ublic disclosure" of patients' information." 562 U.S. at 145. "The [Whalen] Court thus concluded that the statute did not violate 'any right or liberty protected by the Fourteenth Amendment.'" *Id.* (citing *Whalen v. Roe*, 429 U.S. at 606). Second, the Court in *Nelson* relied on the Privacy Act's safeguards to prohibit public disclosure. Third, the Supreme Court in both *Whalen* and in *Nelson* deemed the request for information to be "reasonable."

Here the sensitive voter data sought from the states, including felony convictions and partial SSNs, is on par with the personal information at issue in *Whalen* and *Nelson,* though whether it is "reasonable" is broadly contested by state election officials across the country. *See, e.g.* Editorial, *Texas and Other States Are Right to Refuse Trump Panel's Request for Private Voter Information*, Dallas Morning News (July 7, 2017) ("Conservatives and liberals alike should be appalled that a commission brought into existence by a presidential executive order wants such sensitive personal data on the thinnest of pretexts."). It bears emphasizing that this opposition to

18-F-1517//0903

the Commission's is from a bipartisan group of public officials most expert in the data sought and the laws that apply.

Moreover, contrary to the security methods mandated by the state statute in *Whalen*, the Commission has (1) proposed an unsecure server to receive sensitive data and (2) has disclaimed any responsibility to undertake a Privacy Impact Assessment. Most critically, the Commission has given no indication that its data collection practices are subject to the strictures of the Privacy Act, which was the key reason in *Nelson* that the Court did not reach the informational privacy claim. As Justice Alito explained in the holding for the Court:

> In light of the protection provided by the Privacy Act's nondisclosure requirement, and because the challenged portions of the forms consist of reasonable inquiries in an employment background check, we conclude that the Government's inquiries do not violate a constitutional right to informational privacy.

NASA, 562 U.S. at 764–65.

The Commission has presented this Court with informational privacy risks comparable to those that were before the Supreme Court in *Whalen v. Roe* and *NASA v. Nelson*, but with none of the privacy safeguards or practices that provided the Court with sufficient assurances and little evidence that the request is "reasonable." These are the circumstances where the claim of informational privacy are most compelling. The Supreme Court explained in Whalen that the "interest in avoiding disclosure of personal matters" is an aspect of the right of privacy, and intimated "a sufficiently grievous threat" may establish a "constitutional violation." *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977). Without a "successful effort to prevent abuse and limit access to the personal information at issue," which the disclosure amounts to to "a deprivation of constitutionally protected privacy interests" requiring the state to prove the measures are "necessary to promote a compelling state interest." *Id.* at 607 (Brennan, W., concurring).

If there were any information worthy of a constitutional shield from disclosure, it is personal information shared for the limited purpose of exercising of the right to vote. The right to vote is referenced by the U.S. Constitution five times, more than any other right. U.S. Const. amends. XIV § 5, XV § 1, XIX, XXIV § 1, XXVI § 1. The right to vote, secured only

18-F-1517//0904

through robust voter privacy measures, is foundational to American democracy. That the Commission attempts to collect personal *voter* data en masse raises the constitutional stakes. And, without a "successful effort prevent abuse and limit access to" that data—such as the Commission's direction to use an unsecured website for the data transfer—the state must demonstrate to the Court the "necess[ity]" of the collection "to promote a compelling state interest." *Whalen*, 429 U.S. at 607. A proposal to establish a national database of sensitive voter data, gathered contrary to state privacy law, and with no assurance of privacy protection makes clear the right of informational privacy. There is little in the Supreme Court's decisions in *NASA v. Nelson* and *Whalen v. Roe*, or even the D.C. Circuit's *AFGE* opinion, to suggest otherwise. And regardless of whether the Commission considers itself outside of the FACA or the APA, it is not beyond the reach of the federal Constitution.

The Government has previously survived right to informational privacy challenges where it implemented measures to protect the confidentiality and security of the personal information that it was collecting or there was a federal law that provided substantial protection. *See id.* (upholding collection of personal information by HUD on the SF 85P form); *NASA v. Nelson*, 562 U.S. 134, 156 (2011). But when no such safeguards exist, when the Government has not "evidence a proper concern" for individual privacy, the individual's interest in prohibiting the collection of their information by an agency is strongest. *NASA*, 562 U.S. at 156. That is especially true when the data includes identifying and sensitive information such as addresses, date of birth, SSNs, and political affiliations.

The Commission has taken no steps to protect this sensitive personal information that they are seeking to collect. Instead, they have disclaimed all responsibility for maintaining the security and confidentiality of these records. In the letter to Secretaries of State, Vice Chair Kobach tells the states to "be aware that any documents that are submitted to the full Commission will also be made available to the public." Ex. 3, at 2. The Commission has provided no justification for such broad collection and disclosure of voters' personal information. In the letter, the Vice Chair claims, without any supporting evidence, that the data will be used to "analyze vulnerabilities and

18-F-1517//0905

issues related to voter registration and voting." Ex. 3, at 1. But the Office of the Vice President and the Commission have no authority to oversee state voter registration, and the Executive Order makes clear that the purpose of the Commission is to "study" election integrity.

Informational privacy claims merit heightened scrutiny. *See, e.g.*, *Eisenbud v. Suffolk County*, 841 F.2d 42, 45 (2d Cir. 1988); *Fraternal Order of Police, Lodge 5, v. City of Philadelphia*, 812 F.2d 105, 110 (3d Cir. 1987). This requires a "delicate task of weighing competing interests," *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 578 (3d Cir. 1980). *See Doe v. Attorney General*, 941 F.2d 780 (9th Cir. 1991). In order to overcome the constitutional obligation to protect personal information from disclosure, the government must demonstrate "sufficiently weighty interests in obtaining the information sought" and "justify the intrusions into the individuals' privacy." *AFGE v. HUD*, 118 F.3d at 793. The Commission has not identified any legitimate interests that would justify such a sweeping and unprecedented public disclosure of voter records.

II. EPIC's members will suffer irreparable harm if relief is not granted.

If the Court does not enjoin the Commission's unlawful collection, aggregation, and public disclosure of voter data, EPIC's members will be irreparably harmed. Individual voter data is not broadly available to the public; otherwise there would be no need for the Commission to request it from the states. These records are collected by the states for a specific purpose—voter registration—and voters have not authorized its dissemination to or by the Commission for an entirely different, and undisclosed, purpose.

There is no doubt that the categories of data listed in the Commission's unlawful demand: date of birth, last four digits of the social security number, and political affiliation, paired with full name and address are sensitive and confidential. The unauthorized disclosure of this sensitive personal information would cause immeasurable harm for three reasons. First, a violation of an individual's constitutional rights is a *per se* harm. Second, disclosure of confidential information is a *per se* harm, especially where that disclosure is unlawful and monetary damages are not

18-F-1517//0906

available. And third, creation of a unified federal voter registration database without any privacy or security protections would put members' personal information at risk; voter data has already been targeted at the state level, and the Commission has none of the tools or experience that states have deployed to protect that data from unauthorized access.

A violation of the constitutional right to informational privacy, alone, is sufficient to satisfy the irreparable harm test. *Fort Wayne Women's Health v. Bd. of Comm'rs, Allen County, Ind.*, 735 F. Supp. 2d 1045, 1061 (N.D. Ind. 2010). *See Am. Fed'n of Gov't Emps., AFL-CIO v. Sullivan*, 744 F. Supp. 294, 298 (D.D.C. 1990); *Senior Execs. Ass'n v. United States*, 891 F. Supp. 2d 745, 750–51 (D. Md. 2012). The Commission has made clear that it will publicly release the voter data in some form. First Kobach Decl. ¶ 5. The Commission claims it will "de-identify" this data, but has given "no identification or description of the process or technique, no explanation of what the Commission hopes to protect and how they can ensure they have done so, and no description of the reason for publishing anything." Decl. of Cynthia Dwork ¶ 7, Ex. 23. There is an "inherent contradiction" in the Commission's simultaneous statements that there is no privacy interest in the voter data and that the Commission will take steps to protect the privacy of the data. And the disclosure of personal identifying information itself also gives rise to an irreparable injury. *Does v. Univ. of Wash.*, No. 16-1212, 2016 WL 4147307, *slip op.* at *2 (W.D. Wash. Aug. 3, 2016). "In the age of the internet, when information is made public quickly and without borders, it is nearly impossible to contain an impermissible disclosure after the fact, as information can live on in perpetuity in the ether to be shared for any number of deviant purposes." *Wilcox v. Bastiste*, No. 17-122, 2017 WL 2525309, *slip op.* at *3 (E.D. Wash. June 9, 2017); *see also Pacific Radiation Oncology, LLC v. Queen's Medical Center*, 47 F. Supp. 3d 1069, 1076 (D. Haw. 2014) (noting that it is "beyond dispute that the public disclosure of that information" in medical files would subject patients "to potential irreparable harm").

The unlawful disclosure of confidential or proprietary information is a *per se* harm and should, by itself, justify enjoining the Commission's collection of personal voter data in this case. *See CAIR v. Gaubatz*, 667 F. Supp. 2d 67, 76 (D.D.C. 2009) (granting a temporary restraining

18-F-1517//0907

order to prevent disclosure of CAIR's "proprietary, confidential, and privileged information); *see also Ruckelshaus v. Monsanto Co.*, 463 U.S. 1315, 1317 (1983) (Blackmun, J., in chambers) (denying the government's petition for a stay pending appeal on the grounds that disclosure of Monsanto's proprietary information could "cause irreparable harm"). The Commission cannot seriously contend that disclosure of the voter data elements listed in their June 28, 2017, letter would be permissible under federal or state law, and yet they nevertheless has demanded that the states turn over that confidential voter data.

There is evidence that the Commission will collect the voter data absent an injunction from this court because the state of Arkansas already submitted data via the insecure Department of Defense portal *after this suit was already pending*. TRO Hr'g Tr. 41, July 7, 2017. Arkansas officials have since revealed that the data that they sent to the Commission included "names, addresses, dates of birth, political party affiliations, voter history since 2008, registration status, email addresses and phone numbers." Bill Bowden & Brian Fanney, *U.S. Tells Arkansas to Delete Files on Voter Data*, Arkansas Online (July 13, 2017), Ex. 37. Arkansas did this despite the fact that Governor Asa Hutchinson said that the state should not provide the data " and did not "want to facilitate the providing of that information to a federal database." *Id*. This is clear evidence that the Commission is using its power to influence states to release data that should be kept confidential.

The Commission also cannot credibly claim that they do not intend to collect confidential voter data such as the last four digits of the SSN. In fact, Vice Chair Kobach has used the same data elements that he requested in his June 28, 2017, Commission letter as part of his Kansas-based "Interstate Voter Registration Crosscheck Program." Ex. 33, at 8. The last four digits of the SSN are a core part of the "matching" algorithm used in the Crosscheck program. Yet Kobach's efforts to create a federal Crosscheck program through the Commission's request are designed to circumvent and undermine federal privacy law. Congress passed the Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (Oct. 18, 1988), in order to amend the Privacy Act to limit the improper use of computer matching algorithms by federal

18-F-1517//0908

agencies. Congress passed further amendments to strengthen the due process provisions in the Computer Matching and Privacy Protection Amendments of 1990, Pub. L. No. 101-508, 104 Stat. 1388 (Nov. 5, 1990). Yet Kobach and the Commission now intend to collect voter data to extend their Crosscheck matching program while ignoring the privacy and due process requirements imposed by federal law. This unlawful secondary use of EPIC's members' personal voter data will cause immediate and irreparable harm.

Even the mere collection and aggregation of the state voter data itself would cause an irreparable harm to EPIC's members because the Commission has taken no steps to ensure the security and integrity of the data. States recognize that they face an acute and increasing risk that their voter data will be targeted by malicious hackers and, in response, are taking special measures to protect this sensitive data. *See* Exs. 26–31. Even federal government officials recognize that voter data is uniquely vulnerable due to its sensitive nature and the fact that it is a high value target. *Id.* Yet, despite these clear risks, the Commission intends to put all the eggs in one basket, creating a irresistible target for hackers. The fact that this data will be stored within the EOP does not provide any reassurance. The White House's track record for information security is alarming in its own right. Evan Perez & Shimon Prokupecz, *How the U.S. Thinks Russians Hacked the White House*, CNN (Apr. 8, 2015);[22] Ellen Nakashima, *Hackers Breach Some White House Computers*, Wash. Post (Oct. 28, 2014);[23] Sean Gallagher, *"Hacked" E-Mail Account of White House Worker Exposed in 2013 Password Breach*, ArsTechnica (Sept. 23, 2016);[24] Lily Hay Newman, *That Encrypted Chat App the White House Liked? Full of Holes*, Wired (Mar. 9, 2017).[25] Given the recent history of data breaches in federal government systems

[22] http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.htm.
[23] https://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html.
[24] https://arstechnica.com/security/2016/09/hacked-e-mail-account-of-white-house-worker-exposed-in-2013-password-breach/.
[25] https://www.wired.com/2017/03/confide-security-holes/.

18-F-1517//0909

that house sensitive information, the lack of planning and foresight on the part of the Commission poses an immediate and inexcusable risk to the privacy of all voters.

Not only do the Commission's proposed insecure data transfer methods create serious *security* risks for the sensitive personal voter data that the Commission requested, these methods are incapable of ensuring the *integrity* and accuracy of the data that the Commission receives. The Commission has not provided any evidence that the email address or the File Exchange website are capable of verifying the source and authenticity of the documents and data submitted. Criminals and other unauthorized parties are known to send fake emails "that are made to appear as if they are coming from" government accounts, including accounts within the Pentagon's "Defense Security Service." Jenna McLaughlin, *Pentagon Email Addresses Being Used in Cyber Spoofing Campaign*, Foreign Policy (May 12, 2017).[26] Nothing would stop a malicious actor—perhaps even a foreign government—from submitting fake "voter roll" data to the Commission to degrade the accuracy of the database. These are precisely the types of issues that would have been identified during a Privacy Impact Assessment, but the Commission failed to conduct one prior to initiating this proposed collection.

The Commission goes to great lengths to emphasize that it is only seeking "publicly available" information. But in fact the vast majority of personal data sought by the Commission is protected by state voter privacy laws. According to a preliminary survey by EPIC, states could provide the Commission with little more than name and address of registered voters without running afoul of state law.[27] A study by the Brennan Center also finds numerous restrictions on

---

[26] http://foreignpolicy.com/2017/05/12/pentagon-email-addresses-being-used-in-cyber-spoofing-campaign/.

[27] *See e.g.* Alaska Stat. § 15.07.195 ("The following information set out in state voter registration records is confidential and is not open to public inspection: (1) the voter's age or date of birth; (2) the voter's social security number, or any part of that number; (3) the voter's driver's license number; (4) the voter's voter identification number; (5) the voter's place of birth; (6) the voter's signature."); *see also e.g.* Ind. Code § 3-7-26.4-8 (2017) ("The election division shall not provide information under this section concerning any of the following information concerning a voter: (1) Date of birth. (2) Gender. (3) Telephone number or electronic mail address. (4) Voting history. (5) A voter identification number or another unique field established to identify a voter. (6) The date of registration of the voter.").

18-F-1517//0910

the release of state voter rolls. Brennan Center for Justice, Examples of Legal Risks to Providing Voter Information to Fraud Commission (Jul. 2017).[28]

The Commission contends that it "has only requested data that is already public available," Def. Opp'n 8, and cites to a 2016 report of the National Conference of State Legislatures ("NCSL"). But as the NCSL actually explained, "Generally, all states provide the name and address or the registered voter. From there is gets complicated. At least 25 states limit access to social security numbers, date of birth or other identifying factors such as a drivers license number." *See* National Conference of State Legislatures, States and Election Reform (Feb. 2016).[29] The 2016 NCSL report notes also that "Texas specifically restricts the residential address of any judge in the state" and several states have a general prohibition on "information of a personal nature." *Id.*[30]

The 2016 NCSL report, cited by the Commission, goes on to explain the limitation on access to voter data, use of voter data, and costs for obtaining voter data. The NCSL explains "Beyond candidates and political parties, who can access voter lists varies state by state. Eleven states do not allow members of the public to access voter data." *Id.* at 2. Further, several states restrict the use of voter data. Several states limit "the use to just political purposes or election purposes." *Id.* States also typically charge requesters costs for the production of data. According to the NCSL, "the average cost for a voter list is approximately $1,825."[31]

Even names and address are not always available. The NCSL report notes that "thirty-nine states maintain address confidentiality programs designed to keep the addresses of victims of

---

[28] https://www.brennancenter.org/sites/default/files/analysis/Legal_Implications_of_Kobach_Request.pdf.

[29] http://www.ncsl.org/Documents/Elections/The_Canvass_ February_2016_66.pdf.

[30] *See e.g.* Kan. Stat. Ann. § 45.221(30) (exempting from the Kansas Open Records Act any "Public records containing information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy.").

[31] The Commission made no offer in its letter to the states to pay any of the costs associated with the production of the voter roll data. The Commission instructed the state officials to provide the data by email or to an insecure website.

18-F-1517//0911

domestic violence or abuse, sexual assault or stalking out of public records for their protection." *Id.* at 2. The NCSL describes additional restrictions on the release on name and address information who are preregistered but are also minors. *Id.* at 2-3.

What then to make of a request from a Commission charged with "promoting election integrity" that asks state election officials to turn over Social Security Numbers, military status, felony convictions records, party affiliation and state voting history? The answer is provided by the response of the state officials who simply refused to release the personal data sought by the Commission.

III. The balance of the equities and public interest favor relief.

The balance of the equities and public interest factors favor entry of the temporary restraining order that EPIC seeks. This purpose of temporary relief is to preserve, not "upend the status quo." *Sherley v. Sebelius*, 644 F.3d 388, 398 (D.C. Cir. 2011); *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 43 (2008). Preserving the status quo is the purpose of EPIC's motion. Currently there is no single federal database that houses state voter roll data. The Commission now seeks in an unprecedented shift to change that fact without prior review of the privacy implications as required by law. The public interest and balance of the equities favor EPIC's request to preserve the status quo pending review by this Court.

There are no countervailing interests that weigh against the relief EPIC seeks. The Commission would not be harmed by a temporary halt to its plans, as it has no valid interest in violating the PIA requirements in the E-Government Act. "There is generally no public interest in the perpetuation of unlawful agency action." *League of Women Voters*, 838 F.3d at 12 (citing *Pursuing America's Greatness v. FEC*, 831 F.3d 500, 511-12 (D.C. Cir. 2016); *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013). In fact, "there is a substantial public interest in having governmental agencies abide by the federal laws that govern their existence and operations." *Id.* at 12.

18-F-1517//0912

The Commission's actions cut directly against the stated mission to "identif[y] areas of opportunity to increase the integrity of our election systems." Ex. 3, at 2. By collecting and aggregating detailed, sensitive personal voter information without first conducting a PIA, the Commission is threatening the security and integrity of the entire voting system. This action will not only put voter data at risk; it will risk disincentivizing voters in a way similar to the restrictive documentation requirements in *League of Women Voters*. Indeed, there are already reports of citizens cancelling their voter registration out of concern for their privacy. Andrew Gumbel, *Trump Election Commission Backs Away from Its Request for Voter Data After Outcry*, Guardian (July 13, 2017).[32] The court the found that the requirement to reveal "sensitive citizenship documents" in order to register to vote caused the voter registration numbers to "plummet[]" and found that there was a strong public interest in favor of enjoining the change. *League of Women Voters*, 838 F.3d at 4, 9, 13. The right to vote is "preservative of all rights" and of "most fundamental significance under our constitutional structure." *Id.* at 12. The Commission has not provided any evidence that the collection and aggregation of sensitive voter data would "increase the integrity of our election systems." More likely, it will have the opposite effect.

CONCLUSION

The Emergency Motion for a Temporary Restraining Order should be granted, and Defendants should be restrained from collecting state voter data prior to the completion of a Privacy Impact Assessment.

[32] https://www.theguardian.com/us-news/2017/jul/13/donald-trump-election-integrity-commission-voter-data-backlash.

18-F-1517//0913

Respectfully Submitted,

/s/ Marc Rotenberg
MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel

CAITRIONA FITZGERALD*
EPIC Policy Director

JERAMIE D. SCOTT, D.C. Bar # 1025909
EPIC Domestic Surveillance Project Director

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Plaintiff EPIC

* *Pro hac vice motion pending*

Dated: July 13, 2017

18-F-1517//0914

EPIC v. Commission
No. 17-1320

Exhibits to Plaintiff's Amended Motion for a Temporary Restraining Order and Preliminary Injunction

LIST OF EXHIBITS[1]

Exhibit 1	Exec. Order. No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017)
Exhibit 2	Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017)
Exhibit 3	Letter from Kris Kobach, Vice Chair, Presidential Advisory Commission on Election Integrity, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017)
Exhibit 4	*Perkins v. Dep't of Veteran Affairs*, No. 07-310 (N.D. Ala. Apr. 21, 2010)
Exhibit 5	Memorandum M-03-22 from Josh Bolten, Dir. of Office of Mgmt. & Budget, to Heads of Exec. Dep'ts & Agencies (Sep. 23, 2003)
Exhibit 6	Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Website (July 3, 2017 12:02 AM)
Exhibit 7	Declaration of Kimberly Bryant, EPIC Member (July 5, 2017)
Exhibit 8	Declaration of Julie E. Cohen, EPIC Member (July 5, 2017)
Exhibit 9	Declaration of William T. Coleman III, EPIC Member (July 5, 2017)
Exhibit 10	Declaration of Harry R. Lewis, EPIC Member (July 5, 2017)
Exhibit 11	Declaration of Pablo Garcia Molina, EPIC Member (July 5, 2017)
Exhibit 12	Declaration of Peter G. Neumann, EPIC Member (July 5, 2017)

[1] Exhibits 1–6 were previously filed with EPIC's Emergency Motion. Exhibits 7–17 were previously filed with EPIC's Reply, and have been renumbered for clarity. Exhibit 38 was previously filed with EPIC's Sur-sur-reply, and has been renumbered for clarity. Exhibits 19–24 were previously filed as Supplementary Exhibits 1–7, and have been renumbered for clarity. Exhibit 24 was previously filed as Exhibit 5 with the Second Amended Complaint, and has been renumbered for clarity.

18-F-1517//0915

Exhibit 13	Declaration of Bruce Schneier, EPIC Member (July 5, 2017)
Exhibit 14	Declaration of James Waldo, EPIC Member (July 5, 2017)
Exhibit 15	Declaration of Shoshana Zuboff, EPIC Member (July 5, 2017)
Exhibit 16	National Conference of State Legislatures, *It's a Presidential Election Year: Do You Know Where Your Voter Records Are?* (Feb. 2016)
Exhibit 17	Second (Expert) Declaration of Harry R. Lewis (July 5, 2017)
Exhibit 18	Webpage: Privacy Impact Assessments (PIA), U.S. General Services Administration, (July 7, 2017)
Exhibit 19	U.S. Election Assistance Commission, Office of Inspector General, Final Report. Report No. I-PA- EAC-04-12 (May 2013)
Exhibit 20	Letter from Chris Harvey, Director of Elections, Georgia Secretary of State's Office, to Kris W. Kobach, Vice Chair, Presidential Advisory Commission on Election Integrity (July 3, 2017)
Exhibit 21	Web Article: "SAFE Site facilitates large file transfers", Carlotta Maneice, AMRDEC Public Affairs, The United States Army (April 27, 2015)
Exhibit 22	Privacy Impact Assessment (PIA) for the Safe Access File Exchange ("SAFE"), Department of Defense (2015)
Exhibit 23	Declaration of Cynthia Dwork (July 6, 2017)
Exhibit 24	Letter from Electronic Privacy Information Center (EPIC), to National Association of State Secretaries (July 3, 2017)
Exhibit 25	Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology, 2015 Daily Comp. Pres. Doc. 185 (March 19, 2015)

Exhibit 26	Ass'n for Comput. Machinery, *Statewide Databases of Registered Voters: Study of Accuracy, Privacy, Usability, Security, and Reliability Issues* 6 (Feb. 2006)
Exhibit 27	Testimony of Jeanette Manfra, Acting Deputy Undersecretary for Cybersecurity & Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security (June 21, 2017)
Exhibit 28	Testimony of Michael Haas, Administrator, Wisconsin Elections Commission (June 21, 2017)
Exhibit 29	Statement of Hon. Connie Lawson, Secretary of State, Indiana (June 21, 2017)
Exhibit 30	Statement of Steve Sandvoss, Executive Director, Illinois State Board of Elections (June 21, 2017)
Exhibit 31	Transcript of S. Intel Hearing on Russian Interference in 2016 Election, Panel 1 (June 21, 2017)
Exhibit 32	Transcript of S. Intel Hearing on Russian Interference in 2016 Election, Panel 2 (June 21, 2017)
Exhibit 33	Sec'y of State, Kansas, *Interstate Crosscheck Program Grows* (2013)
Exhibit 34	Presentation by Kris W. Kobach to the National Ass'n of State Election Dirs., *Interstate Voter Registration Crosscheck Program* (Jan. 26, 2013)
Exhibit 35	Greg Palast, *The GOP's Stealth War Against Voters*, Rolling Stone (Aug. 24, 2016)
Exhibit 36	U.S. Digital Serv., *Report to Congress — December 2016* (2016)
Exhibit 37	Bill Bowden & Brian Fanney, *U.S. Tells Arkansas to Delete Files on Voter Data*, Arkansas Online (July 13, 2017)
Exhibit 38	Declaration of Marc Rotenberg (July 7, 2017)

Exhibit 39 Andrew Gumbel, *Trump Election Group Backs Away From its Request for Voter Data After Outcry*, The Guardian (July 13, 2017)

Exhibit 40 *Arkansas Voter Registration Data*, Office of the Secretary of State of Arkansas (March 14, 2011)

18-F-1517//0918

Exhibit 1

Federal Register
Vol. 82, No. 93
Tuesday, May 16, 2017

Presidential Documents

Title 3—

The President

Executive Order 13799 of May 11, 2017

Establishment of Presidential Advisory Commission on Election Integrity

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to promote fair and honest Federal elections, it is hereby ordered as follows:

Section 1. *Establishment.* The Presidential Advisory Commission on Election Integrity (Commission) is hereby established.

Sec. 2. *Membership.* The Vice President shall chair the Commission, which shall be composed of not more than 15 additional members. The President shall appoint the additional members, who shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience that the President determines to be of value to the Commission. The Vice President may select a Vice Chair of the Commission from among the members appointed by the President.

Sec. 3. *Mission.* The Commission shall, consistent with applicable law, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President that identifies the following:

(a) those laws, rules, policies, activities, strategies, and practices that enhance the American people's confidence in the integrity of the voting processes used in Federal elections;

(b) those laws, rules, policies, activities, strategies, and practices that undermine the American people's confidence in the integrity of the voting processes used in Federal elections; and

(c) those vulnerabilities in voting systems and practices used for Federal elections that could lead to improper voter registrations and improper voting, including fraudulent voter registrations and fraudulent voting.

Sec. 4. *Definitions.* For purposes of this order:

(a) The term "improper voter registration" means any situation where an individual who does not possess the legal right to vote in a jurisdiction is included as an eligible voter on that jurisdiction's voter list, regardless of the state of mind or intent of such individual.

(b) The term "improper voting" means the act of an individual casting a non-provisional ballot in a jurisdiction in which that individual is ineligible to vote, or the act of an individual casting a ballot in multiple jurisdictions, regardless of the state of mind or intent of that individual.

(c) The term "fraudulent voter registration" means any situation where an individual knowingly and intentionally takes steps to add ineligible individuals to voter lists.

(d) The term "fraudulent voting" means the act of casting a non-provisional ballot or multiple ballots with knowledge that casting the ballot or ballots is illegal.

Sec. 5. *Administration.* The Commission shall hold public meetings and engage with Federal, State, and local officials, and election law experts, as necessary, to carry out its mission. The Commission shall be informed by, and shall strive to avoid duplicating, the efforts of existing government entities. The Commission shall have staff to provide support for its functions.

18-F-1517//0920

Sec. 6. *Termination*. The Commission shall terminate 30 days after it submits its report to the President.

Sec. 7. *General Provisions*. (a) To the extent permitted by law, and subject to the availability of appropriations, the General Services Administration shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis.

(b) Relevant executive departments and agencies shall endeavor to cooperate with the Commission.

(c) Insofar as the Federal Advisory Committee Act, as amended (5 U.S.C. App.) (the "Act"), may apply to the Commission, any functions of the President under that Act, except for those in section 6 of the Act, shall be performed by the Administrator of General Services.

(d) Members of the Commission shall serve without any additional compensation for their work on the Commission, but shall be allowed travel expenses, including per diem in lieu of subsistence, to the extent permitted by law for persons serving intermittently in the Government service (5 U.S.C. 5701–5707).

(e) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(g) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,
May 11, 2017.

[FR Doc. 2017–10003
Filed 5–15–17; 8:45 am]
Billing code 3295–F7–P

18-F-1517//0921

Exhibit 2

the WHITE HOUSE

From the Press Office

Speeches & Remarks

Press Briefings

Statements & Releases

Nominations & Appointments

Presidential Actions

Legislation

Disclosures

The White House
Office of the Vice President

For Immediate Release June 28, 2017

Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity

This morning, Vice President Mike Pence held an organizational call with members of the Presidential Advisory Commission on Election Integrity. The Vice President reiterated President Trump's charge to the commission with producing a set of recommendations to increase the American people's confidence in the integrity of our election systems.

"The integrity of the vote is a foundation of our democracy; this bipartisan commission will review ways to strengthen that integrity in order to protect and preserve the principle of one person, one vote," the Vice President told commission members today.

The commission set July 19 as its first meeting, which will take place in Washington, D.C.

18-F-1517//0923

Vice Chair of the Commission and Kansas Secretary of State Kris Kobach told members a letter will be sent today to the 50 states and District of Columbia on behalf of the Commission requesting publicly-available data from state voter rolls and feedback on how to improve election integrity.

18-F-1517//0924

Exhibit 3

Presidential Advisory Commission on Election Integrity

June 28, 2017

The Honorable Elaine Marshall
Secretary of State
PO Box 29622
Raleigh, NC 27626-0622

Dear Secretary Marshall,

I serve as the Vice Chair for the Presidential Advisory Commission on Election Integrity ("Commission"), which was formed pursuant to Executive Order 13799 of May 11, 2017. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President of the United States that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine the American people's confidence in the integrity of federal elections processes.

As the Commission begins it work, I invite you to contribute your views and recommendations throughout this process. In particular:

1. What changes, if any, to federal election laws would you recommend to enhance the integrity of federal elections?
2. How can the Commission support state and local election administrators with regard to information technology security and vulnerabilities?
3. What laws, policies, or other issues hinder your ability to ensure the integrity of elections you administer?
4. What evidence or information do you have regarding instances of voter fraud or registration fraud in your state?
5. What convictions for election-related crimes have occurred in your state since the November 2000 federal election?
6. What recommendations do you have for preventing voter intimidation or disenfranchisement?
7. What other issues do you believe the Commission should consider?

In addition, in order for the Commission to fully analyze vulnerabilities and issues related to voter registration and voting, I am requesting that you provide to the Commission the publicly-available voter roll data for North Carolina, including, if publicly available under the laws of your state, the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social

security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.

You may submit your responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE"), which is a secure FTP site the federal government uses for transferring large data files. You can access the SAFE site at https://safe.amrdec.army.mil/safe/Welcome.aspx. We would appreciate a response by July 14, 2017. Please be aware that any documents that are submitted to the full Commission will also be made available to the public. If you have any questions, please contact Commission staff at the same email address.

On behalf of my fellow commissioners, I also want to acknowledge your important leadership role in administering the elections within your state and the importance of state-level authority in our federalist system. It is crucial for the Commission to consider your input as it collects data and identifies areas of opportunity to increase the integrity of our election systems.

I look forward to hearing from you and working with you in the months ahead.

Sincerely,

Kris Kobach

Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity

Exhibit 4

FILED
2010 Apr-21 PM 03:15
U.S. DISTRICT COURT
N.D. OF ALABAMA

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

JIM HENRY PERKINS and JESSIE FRANK QUALLS, on their own behalf and on the behalf of all others similarly situated,

Plaintiffs,

v. **CV No. 2:07-310-IPJ**

UNITED STATES DEPARTMENT OF VETERANS AFFAIRS; et al.

Defendants.

MEMORANDUM OPINION

This case is before the court upon remand from the Eleventh Circuit to conduct a "claim-by-claim" analysis to determine the validity of plaintiffs' remaining challenges brought under the Administrative Procedures Act ("APA"), 5 U.S.C. § 551 *et seq.*, and seeking to enforce provisions of the Privacy Act, 5 U.S.C. § 552a; the E-Government Act of 2002, 44 U.S.C. § 3501 note; and the Veterans Benefits, Health Care, and Information Technology Act of 2006, 38 U.S.C. § 5724. Only counts two, five, six, and eight remain, and the court examines each claim in turn.

Factual Background

On January 22, 2007, an employee of the U.S. Department of Veterans

18-F-1517//0929

Affairs ("VA") reported an external hard drive containing personally identifiable information and individually identifiable health information of over 250,000 veterans was missing from the Birmingham, Alabama Medical Center's Research Enhancement Award Program ("REAP"). VA Office of Inspector General ("OIG") Report, at 7. The IT Specialist responsible for the external hard drive, "John Doe," used the hard drive to back up data on his computer and other data from a shared network drive.[1] The hard drive is thought to contain the names, addresses, social security numbers ("SSN"), dates of birth, phone numbers, and medical files of hundreds of thousands of veterans and also information on more than 1.3 million medical providers. VA OIG Report at 7, 9 (doc. 33-2). To date, it has not been recovered.

John Doe was an IT Specialist working for the Birmingham REAP, a program that focused on "changing the practices of health care providers to ensure that they provide the latest evidence-based treatment, and on using VA databases

---

[1]The REAP Director approved the purchase of external hard drives as a means to provide more space to the Medical Center's near-full server. VA OIG Report, at 15. No policy required the protection of sensitive data on removable computer storage devices unless such devices were to be carried outside a VA facility. *Id.* at 16. The REAP Director claimed the Information Security Officer ("ISO") conferred with him in making the decision to purchase the external hard drives, but the ISO claimed he was not involved and did not know of the need for additional server space. The VA OIG concluded no one made a timely request to the ISO for additional space. VA OIG Report, at 15.

18-F-1517//0930

to link the care of VA patients to more general information on the population as a whole." *Id.* at 3. To reach these goals, the Birmingham REAP collects data on patients and medical providers from multiple sources for dozens of separate research projects." *Id.* The Data Unit of the Birmingham REAP was comprised of the Data Unit Manager, three IT Specialists, and two student program support Assistants. *Id.* at 4. John Doe worked "with national VA databases and design[ed] statistical programs to support Birmingham REAP research projects." *Id.*

The VA OIG identified three projects for which John Doe was conducting research. The first "involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medication to improve glucose levels, cholesterol, and blood pressure"; the second "involved examining the quality of care to patients following myocardial infarction . . ., and attempted to determine whether certain demographic characteristics of the medical providers, such as their age, impacted the care rendered to these patients"; and the third "involved using a patient survey to identify use of over-the-counter medications in patients taking prescription medications and link the information obtained to various VA databases to determine whether patients suffered any adverse effects from the combination of medications." *Id.* at 22, 25, 30. In gathering the information needed to complete these projects, John Doe improperly received

18-F-1517//0931

access to various databases and stores of information, and various components of the VA improperly released information to John Doe or gave John Doe such access. *Id.* at 22-33. He was therefore able "to accumulate and store vast amounts of individually identifiable health information that was beyond the scope of the projects he was working on. [The OIG] believe[s] much of this information was stored on the missing external hard drive." *Id.* at 22. Accurate reporting of what information was on the external hard drive has been difficult because the hard drive is still missing; John Doe encrypted or deleted multiple files from his computer after reporting the data missing; and John Doe was not initially forthright with criminal investigators. *Id.* at ii.

After John Doe reported the missing hard drive on January 22, 2007, the VA Security Operations Center ("SOC") was immediately notified. *Id.* at 7. The SOC wrote a report and provided it to the VA OIG on January 23, 2007; on that same day, an OIG criminal investigator came to the Birmingham VAMC and conducted an interview. The Federal Bureau of Investigation became involved in the investigation on January 24, 2007. A forensic analysis of John Doe's computer began on January 29, 2007, and on February 1, 2007, the OIG began to analyze what data could have been on the missing hard drive. *Id.* at 8, 9. Press releases dated on February 2 and 10, 2007, discussed the loss of the hard drive and the information it contained.

18-F-1517//0932

> Subsequent to the reported loss of the Birmingham REAP data but prior to receiving the results of the OIG analysis of this data on February 7, 2007, VA senior management concluded that anyone whose SSN was thought to be contained in any of the missing files, irrespective of the ability of anyone possessing this data to match an SSN with a name or any other personal identifier, should be notified and offered credit protection. The basis for this decision was a memorandum issued on November 7, 2006. . . . The memorandum states that "in the event of a data loss involving individual and personal information. . . VA officials have a responsibility to notify the individual(s) of the loss in a timely manner and to offer these protection services."

Id. at 11. The VA sent letters to those individuals whose information was thought to be compromised by the data breach, which gave them the option of one year of free credit monitoring services. *Id.* at 12.

The VA had also requested the Department of Health and Human Services to perform a risk analysis focusing on the Centers for Medicaid and Medicare Services ("CMS") data involved in the breach. *Id.* The missing external hard drive contained approximately 1.3 million health care providers' information,

18-F-1517//0933

including the SSNs of 664,165 health care providers. *Id.* On March 28, 2007, the CMS Chief Information Officer and Director sent a letter to the VA Assistant Secretary for Office of Information and Technology that stated, based on the CMS's completed independent risk analysis:

> [T]here is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned. The letter requested that "VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file."

Id. From April 17 to May 22, 2007, the VA sent notification letters to the 1.3 million health care providers. *Id.* By May 31, 2007, it sent additional letters offering one year of credit monitoring to the 664,165 health care providers whose SSNs appeared to be on the hard drive. VA OIG Report, at 12.

Analysis

A valid claim under the APA must attack agency action, which is defined as "includ[ing] the whole or a part of an agency rule, order, license, sanction, relief or the equivalent or denial thereof, or failure to act." *Fanin v. U.S. Dep't of*

18-F-1517//0934

Veterans Aff., 572 F.3d 868, 877 (11th Cir. 2009) (citing 5 U.S.C. § 551(13)).

> If the claim attacks an agency's action, instead of failure to act, and the statute allegedly violated does not provide a private right of action, then the "agency action" must also be a "final agency action." [5 U.S.C. § 704; *see also Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 61-62, 124 S.Ct. 2373, 2379 (2004)]. "To be considered 'final,' an agency's action: (1) must mark the consummation of the agency's decisionmaking process–it must not be of a merely tentative or interlocutory nature; and (2) must be one by which rights or obligations have been determined, or from which legal consequences will flow. *U.S. Steel Corp. v. Astrue*, 495 F.3d 1272, 1280 (11th Cir. 2007)(quoting *Bennett v. Spear*, 520 U.S. 154, 177-78, 117 S.Ct. 1154, 1168 (1997)).

Id. However, if the claim challenges a failure to act, the court may compel "agency action unlawfully withheld or unreasonably delayed. . . only where a plaintiff asserts that an agency failed to take a *discrete* agency action that it is *required* to take." *Id.* at 877-878 (citing *Norton*, 542 U.S. at 64) (emphasis in original).

Further, the court notes the remaining claims seek only injunctive and

declaratory relief. Such relief may be granted only if the plaintiffs demonstrate that they are "likely to suffer future injury." *City of Los Angeles v. Lyons*, 461 U.S. 95, 105, 103 S.Ct. 1660, 1667 (1983); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564, 112 S.Ct. 2130, 2138 (1992) (citing *Lyons*, 461 U.S. at 102) ("'Past exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief.'"); *Seigel v. LePore*, 234 F.3d 1163, 1176-77 (11th Cir. 2000) (*en banc*) ("As we have emphasized on many occasions, the asserted irreparable injury "must be neither remote nor speculative, but actual and imminent.") (citations omitted). *Emory v. Peeler*, 756 F.2d 1547, 1552 (11th Cir. 1985) (To grant declaratory relief, "there must be a substantial continuing controversy between parties having adverse legal interests. The plaintiff must allege facts from which the continuation of the dispute may be reasonably inferred. Additionally, the continuing controversy . . . must be real and immediate, and create a definite, rather than speculative threat of future injury.").

Count Two

The plaintiffs claim that the VA failed "to create and maintain an accounting of the date, nature, and purpose of its disclosures" pursuant to the Privacy Act, 5 U.S.C. § 552a(c)(1), when John Doe accessed VA files to complete

VA projects. Joint Status Report ("JSR"), at 8 (doc. 56). The Privacy Act requires

> [e]ach agency, with respect to each system of records under its control, shall–
>
> (1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of–
>
> (A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and
>
> (B) the name and address of the person or agency to whom the disclosure is made. . .

5 U.S.C. § 552a(c)(1). Under the exception provided in subsection (b)(1), agencies need not provide an accounting for disclosures made to "officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). Accordingly, to the extent John Doe needed the information that he accessed to perform his duties, the VA had no obligation to account.

To the extent John Doe had no need for the information contained on the external hard drive in the performance of his duties, the plaintiffs must show the disclosure was pursuant to one of the provisions in 5 U.S.C. § 552a(b)(3)-(12).

18-F-1517//0937

See 5 U.S.C. § 552a(c)(1)(A). After failing to argue in the JSR that any of those subsections apply, plaintiffs now claim that the VA's disclosure to John Doe falls under 5 U.S.C. § 552a(b)(5), which requires accounting when the disclosure is "to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable."

However, the accounting requirement in 5 U.S.C. § 552a(b)(5) is not triggered by the activity at issue in this case. An accounting is required only upon a disclosure to a recipient described in that subsection. Although "recipient" is not defined in the Privacy Act, it does not stand to reason that an agency that maintains records needed by one of its own researchers to fulfill his duties would be required to provide *itself* with "advance adequate written assurance that the record will be used solely as a statistical research or reporting record." Indeed, pertinent legislative history and Office of Management and Budget ("OMB") regulations suggest that an accounting was only intended when the disclosures were to individuals or agencies outside the agency maintaining the record. *See* S. REP. NO. 93-1183 (1974) *reprinted in* U.S. CODE CONGRESSIONAL AND ADMINISTRATIVE NEWS, 6916, 6967 (stating that subsection 201(b)(4) "[r]equires any federal agency that maintains a personal information system or file to maintain an accurate accounting of the date, nature, and purpose of nonregular access

granted to the system, and each disclosure of personal information made to any person *outside the agency, or to another agency. . . .*") (emphasis added); H.R. No. 93-1416, 2 (describing the summary and purpose of the Act as "requir[ing] agencies to keep an accounting of transfers of personal records *to other agencies and outsiders*"); 40 Fed. Reg. 28955 (July 9, 1975) (differentiating between "agencies disclosing records" and "recipient agencies" in the context of 5 U.S.C. § 552a(b)(5)).

Even if subsection (b)(5) is applicable in this case, the plaintiffs argue only that John Doe gave an advance adequate written assurance before accessing information from only one database, the Veterans Integrated Service Network ("VISN") 7 Data Warehouse. Plaintiff's Response (doc. 64) at 4. Accordingly, subsection (b)(5) applies only for John Doe's access to the VISN 7 Data Warehouse to perform research for "Project 1," which involved diabetes management research. *See* VA OIG Report, at 22. Moreover, the plaintiffs cannot show that any failure to account for John Doe's access to the VISN 7 Data Warehouse to research diabetes management is causing them harm. Although the plaintiffs are upset about the loss of their personal information and the prospect of potential credit fraud in the future, any accompanying harm is attributable to the

18-F-1517//0939

loss of the information in the first place, *not* the purported failure to account.[2] Thus, even assuming *arguendo* that 5 U.S.C. § 552a(b)(5) applies, the plaintiffs cannot show that the alleged harm is fairly traceable to the VA's conduct, a deficiency fatal to their claim. *See Allen v. Wright*, 468 U.S. 737, 753 & n.19, 104 S.Ct. 3315, 3325 & n.19 (1984) (plaintiffs do not have standing where they failed to allege injuries that are caused by the defendants).

Because of these sufficient and independent reasons, the plaintiffs have not shown that the VA failed to take discrete agency action that it was required to take. Accordingly, the court finds that the plaintiffs have failed to state a claim upon which relief can be granted, and Count Two is due to be **DISMISSED**.

---

[2]The plaintiffs urge, "The Veterans have a right to know what information [was on the hard drive]. They deserve to know the 'purpose' for which John Doe was using the information," Plaintiff's Response, at 8 (doc. 64). However, the VA OIG report details, to the extent determinable, the information on the hard drive and the purpose for which John Doe was accessing the information. The VA OIG Report states that the hard drive is believed to contain "personally identifiable information and/or individually identifiable health information for over 250,000 veterans, and information obtained from the [CMS], on over 1.3 million medical providers." VA OIG Report, at i. Moreover, it was difficult for the VA to make such a determination, as John Doe was not candid when he was interviewed; he deleted or encrypted files from his computer after the hard drive went missing; and he tried to hide the extent, magnitude, and impact of the missing data. *Id.* at ii. Lastly, the plaintiffs know that the purpose John Doe was accessing the VISN 7 Data Warehouse was related to his research for "Project 1," *id.* at 22-23, which "involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medication to improve glucose levels, cholesterol, and blood pressure," VA OIG Report, at 22.

18-F-1517//0940

Count Five

Count Five involves the VA's alleged failure to establish appropriate safeguards in violation of the Privacy Act, 5 U.S.C. § 552a(e)(10). The plaintiffs have failed to argue that the alleged conduct of the VA constituted a failure of discrete agency action that the VA was required to take, but request that Count Five "move forward as detailed in the Plaintiffs' Statement in the Joint Report." Plaintiff's Brief, at 13 (doc. 64). In the Joint Status Report, the plaintiffs devote just over one page to briefing this issue and cite 5 U.S.C. § 552a(e)(10),[3] arguing that the VA failed to enforce this subsection in the numerous ways listed in their complaint.[4] Joint Status Report ("JSR"), at 10-11 (doc. 56). The plaintiffs then

---

[3]5 U.S.C. § 552a(e)(10) requires the VA to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

[4]Plaintiffs cite specifically to paragraph 80 of the Second Amended Complaint (doc. 21), which states:

> Among other things, Defendants' failures include operating a computer system or database from which an employee, including John Doe, can download or copy information, like the Personal Information and the Medical Information, onto the VA External Hard Drive without proper encryption and when not necessary to perform his or her duties; failing to conduct a data access inventory for John Doe and other VA employees and contractors with access to the VA's office at the Pickwick Conference Center; failing to provide software that would require or enable encryption of data downloaded or copied

18-F-1517//0941

ask the court for an injunction forcing full implementation and compliance "with Handbook 6500 and other procedures and policies put in place in Birmingham by the VA in response to this incident, to conduct an independent audit of its compliance, and to file that audit with the court." Plaintiff's Response, at 14 (doc. 64) (footnotes added). Such an injunction is untenable.

Handbook 6500 is a seventy-one page (seven appendices excluded) document that details the responsibilities of almost two dozen information security personnel and dozens of policies and procedures. As pointed out by the defense, policies explained in the Handbook include maintaining the temperature in the building and proper use of the facsimile machines. In addition, the "other procedures and policies" put in place at the Birmingham facility are also

---

> to mobile hard drives and devices, like the VA External Hard Drive from VA computers and databases at the VA offices and facilities in the Birmingham, Alabama area; failing to secure the VA External Hard Drive under lock and key when not in the immediate vicinity of John Doe; failing to house and protect the VA External Hard Drive to reduce the opportunities for unauthorized access, use, or removal; failing to provide intrusion detection systems at the VA office at the Pickwick Conference Center; failing to store the VA External Hard Drive in a secure area that requires proper escorting for access; failing to require and conduct appropriate background checks on all VA employees and contractors with access to the VA Office in the Pickwick Conference Center; and failing to protect against the alienation and relinquishment of control over the VA External Hard Drive, causing the Personal Information and Medical Information to be exposed to unidentified third parties.

Second Amended Complaint (doc. 21), ¶ 80.

18-F-1517//0942

numerous. *See e.g.*, VA Directive 6504 (doc. 61-3) (governing the transmission, transportation and use of, and access to, VA data outside VA facilities); VA Handbook 6500, at 7 (doc. 61-4) (a seventy-one page document "establish[ing] the foundation for VA's comprehensive information security program and its practices that will protect the confidentiality, integrity, and availability of information"); Medical Center Memo 00-ISO-02 (doc. 61-5) ("assign[ing] responsibility and establish[ing] procedures for managing computer files at the Birmingham VA Medical Center"); Medical Center Memo 00-ISO-05 (doc. 61-6) (requiring VA employees at the Medical Center to get permission before use of removable storage media, especially Universal Serial Bus ("USB") devices, and requiring written permission for the removal of sensitive information from VA facilities); Information Security Program VISN 7 AIS Operational Security Policy (doc. 61-9) (establishing procedures to implement a "structured program to safeguard all IT assets"); Memorandum 10N7-077 of VISN 7 VA Southeast Network (doc. 61-10) (stating "It is the policy of VISN 7 that no sensitive information ([personal health information or personal identifiable information]) will be stored on the storage media of any device without encryption or where the device is not *physically secured* to prevent accidental loss of sensitive information in the event of theft") (emphasis in original).

Cases that suggest a broad injunction enforcing all of these policies is

18-F-1517//0943

appropriate are "relic[s] of a time when the federal judiciary thought that structural injunctions taking control of executive functions were sensible. That time has past." *Rahman v. Chertoff*, 530 F.3d 622, 626 (7th Cir. 2008). "The limitation to discrete agency action precludes the kind of broad programmatic attack [the Supreme Court] rejected in *Lujan v. National Wildlife Federation*, 497 U.S. 871, 110 S.Ct 3177, 111 L.Ed.2d 695 (1990)." *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 64, 124 S.Ct. 2373, 2379-2380 (2004); *see Lujan*, 497 U.S. at 891 When presented with similar circumstances in *Lujan*, the Supreme Court responded:

> Respondent alleges that violation of the law is rampant within this program-failure to revise land plans in proper fashion, failure to submit certain recommendations to Congress, failure to consider multiple use, inordinate focus upon mineral exploitation, failure to provide required public notice, failure to provide adequate environmental impact statements. Perhaps so. But respondent cannot seek *wholesale* improvement of this program by court decree, rather than in the office of the Department or the halls of Congress, where programmatic improvements are normally made.

Lujan, 497 U.S. at 891. Courts are not empowered to compel "compliance with

broad statutory mandates," *Norton*, 542 U.S. at 66-67, nor can they engage in general review of an agency's day-to-day operations to ensure such compliance. *Id.*; *Lujan*, 497 U.S. at 899.

Even if this court could pass on such a generalized challenge, the court is convinced that Count Five is moot.

> "'[A] case is moot when the issues presented are no longer "live" or the parties lack a legally cognizable interest in the outcome.' " *County of Los Angeles v. Davis,* 440 U.S. 625, 631, 99 S.Ct. 1379, 59 L.Ed.2d 642 (1979) (quoting *Powell v. McCormack,* 395 U.S. 486, 496, 89 S.Ct. 1944, 23 L.Ed.2d 491 (1969)). The underlying concern is that, when the challenged conduct ceases such that " 'there is no reasonable expectation that the wrong will be repeated,' " *United States v. W.T. Grant Co.,* 345 U.S. 629, 633, 73 S.Ct. 894, 97 L.Ed. 1303 (1953), then it becomes impossible for the court to grant " 'any effectual relief whatever' to [the] prevailing party," *Church of Scientology of Cal. v. United States,* 506 U.S. 9, 12, 113 S.Ct. 447, 121 L.Ed.2d 313 (1992) (quoting *Mills v. Green,* 159 U.S. 651, 653, 16 S.Ct. 132, 40 L.Ed. 293 (1895)).

City of Erie v. Pap's A.M., 529 U.S. 277, 287, 120 S.Ct. 1382, 1390 (2000).

Because the evidence submitted to the court shows that new security procedures and policies have been implemented and the deficiencies revealed in the VA OIG Report have been remedied, there is no "live" issue for which this court can grant effectual relief.

Count Six

In Count Six, the plaintiffs claim that the VA failed to perform a privacy impact assessment ("PIA") pursuant to the E-Government Act of 2002 when it procured the external hard drives. Pursuant to the E-Government Act, agencies must perform a PIA before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form." 44 U.S.C. § 3501 note (E-Government Act of 2002, § 208(b)(1)(A)). The definition of "information technology" includes "any equipment or interconnected system . . . used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly . . . ." 40 U.S.C. § 11101(6); *see* 44 U.S.C. § 3501 note, § 201 (applying definitions from 44 U.S.C. §§ 3502, 3601); 44 US.C. § 3502(9) (applying the definition of 40 U.S.C. § 11101(6)). The disputed issue is whether the purchase of the external hard drives triggered the duty to perform a PIA.

The plaintiffs claim that the inclusion of "any equipment" in the definition of information technology brings the hard drives within the meaning of the term, thereby requiring the PIA. However, such an interpretation is implausible, as it would require government agencies that maintain personal information on individuals to conduct or update a PIA each time it purchases any computer, monitor, router, telephone, calculator, or other piece of equipment involved in a system that stores, analyzes, or manages the data. Rather, the purchase of several external hard drives, seems to be a "minor change[] to a system or collection that do[es] not create new privacy risks," and therefore does not require a PIA. *See* M-03-22, Attachment A 2.B.3.g., Office and Management and Budget ("OMB") Guidance Implementing the Privacy Provisions of the E-Government Act of 2002, at Section II.B.3.f (doc. 61-15) (hereinafter "M-03-22").

Lending support to this interpretation is the fact that PIAs are required to address (1) what information is collected and why, (2) the agency's intended use of the information, (3) with whom the information would be shared, (4) what opportunities the veterans would have to decline to provide information or to decline to share the information, (5) how the information would be secured, and (6) whether a system of records is being created. *See* 44 U.S.C. § 3501 note (E-Government Act of 2002, § 208(b)(2)(B)); M-03-22, at Section II.C.1.a. These types of inquiries are certainly appropriate and required when the VA initially

18-F-1517//0947

created the Birmingham VAMC system and began collecting data, but not where already collected and stored data is simply being transferred from a server to an external hard drive. The factors above are not relevant for such a transfer and a new PIA would not be informative of what information is being collected, the intended use of the information, or with whom the information would be shared. Under such circumstances, Congress surely did not intend a PIA to be performed.

To the extent the plaintiffs argue that security procedures were not followed or hardware security protocols were breached at the VA facility in Birmingham when the external hard drive went missing, such claims are not actionable under the E-Government Act of 2002. Rather, those arguments should have been pursued pursuant to the Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541 *et seq.*, a claim that the plaintiffs waived after not pursuing it on appeal. *Fanin v. U.S. Dep't of Veterans Affairs*, 572 F.3d 868, 876 n.1.

Count 8

The final count before the court involves the VA's alleged failure to perform an independent risk analysis ("IRA") to determine the risk presented by the loss of the hard drive pursuant to the Veterans Benefits, Health Care, and Information Technology Act of 2006 (VBHCITA), 38 U.S.C. § 5724(a)(1). The plaintiffs also claim that the VA acted unreasonably by providing only one year of credit monitoring services.

18-F-1517//0948

The VBHCITA[5] provides:

> In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall ensure that, as soon as possible after the data breach, a non-Department entity or the Office of Inspector General of the Department conducts an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.

38 U.S.C. § 5724(a)(1).

After John Doe reported the missing hard drive on January 22, 2007, the VA launched an immediate investigation that culminated in the decision to offer one year of free credit monitoring services for 198,760 living individuals whose information was contained on the hard drive. VA OIG Report, at 12. The VA made this decision *before* the completion of the IRA conducted by the Centers for Medicaid & Medicare Services ("CMS"). On February 7, 2007, VA senior

---

[5]The VBHCITA became effective December 22, 2006. The data breach incident at issue occurred on January 22, 2007. The VA passed regulations that became effective June 22, 2007, six months after the passage of the VBHCITA and five months after the loss of the external hard drive.

18-F-1517//0949

management decided that anyone whose SSN was on the hard drive should be notified and offered credit protection. *Id.* at 11. Approximately one and one-half months later, on March 28, 2007, the CMS Chief Information Officer and Director stated that based on the IRA, "There is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned." *Id.* at 12. He recommended that the "VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file." *Id.* Notification letters were sent out to the health care providers by May 31, 2007. *Id.*

Thus, the VA proactively assumed that the veterans were at risk and provided the remedy provided in the statute[6] *before* it had confirmation from the IRA that such a remedy was appropriate under the circumstances. By presuming a reasonable risk of harm from the disclosure of personally identifiable information and providing credit protection services required when an IRA reveals a "reasonable risk" of harm, *see* 38 U.S.C. § 5724(a)(2), the VA has provided the

---

[6]In addition, VA regulations limit credit monitoring awarded to those who are subject to a reasonable risk for misuse of sensitive personal information to one year. 38 C.F.R. § 75.118(a).

18-F-1517//0950

plaintiffs with any relief they are due.[7] Indeed, the IRA conducted by CMS affirmed the propriety of the relief offered by the VA.

Despite having been given such relief, the plaintiffs insist the IRA was insufficient and urge an additional IRA focusing on the veterans must be completed. However, the statute does not require an *individual* risk analysis as the plaintiffs state in their JSR, *See* JSR, at 12-13, 15, only an *independent* risk analysis.[8] The VA OIG Report contains multiple groups of individuals whose private information was compromised: veterans, VA OIG Report, at 7; physicians, *id.* at 10; deceased physicians, *id.*; other health care providers, *id.*; non-veteran, non-VA employees, *id.* at 24; and VA employees, *id.* Furthermore, some veterans were only identified by their SSNs; others were identified by SSNs and dates of birth; others by their name, SSN, and medical information; and others identified

---

[7] The plaintiffs offer a General Accountability Office report that states that a May 5, 2006, incident involving a missing tape with sensitive information of thousands of individuals on it warranted "credit protection and data breach analysis for 2 years." JSR, at 14. As the plaintiffs explain, however, only one year of credit protection was offered, while two years of breach analysis was given. Declaration of Michael Hogan ("Hogan Decl."), ¶¶ 2 (doc. 61-19) and Attachment A (doc. 61-20).

[8]The plaintiffs' argument that the CMS was an inappropriate entity to perform the IRA has no merit, as the statute requires either the VA OIG or a non-Department [of Veterans Affairs] entity to conduct the IRA. 38 U.S.C. § 5724(a)(1). The CMS is under the purview of the Department of Health and Human Services.

by various combinations of seven fields of identifying information. *Id.* at 9. The health care providers are identified on the hard drive by different combinations of forty-eight different fields of data. *Id.* at 10. All of this information was on a single external hard drive lost during a single data breach. The statute only requires an "independent risk analysis of the data breach," not multiple IRAs for each group of individuals whose information was compromised. *See* 38 U.S.C. § 5724(a)(1).

Because the plaintiffs were awarded appropriate relief and because the VA conducted an adequate IRA of the data breach, the court finds that the VA did not fail to take agency action it was required to take with respect to count eight.

Conclusion

Having considered the foregoing and being of the opinion that the plaintiffs have failed to properly state any claims challenging final agency action under the Administrative Procedures Act, 5 U.S.C. § 551 *et seq.*, the court finds that Counts Two, Five, Six, and Eight shall be **DISMISSED**. The court shall so rule by separate order.

DONE and **ORDERED**, this the 21st day of April 2010.

INGE PRYTZ JOHNSON
U.S. DISTRICT JUDGE

18-F-1517//0952

Exhibit 5

This is historical material, "frozen in time" and not current OMB guidance.
The web site is no longer updated and links to external web sites and some internal pages will not work.

OFFICE OF
MANAGEMENT AND BUDGET

September 26, 2003

M-03-22

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
DirectoR

SUBJECT: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

The attached guidance provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

The Administration is committed to protecting the privacy of the American people. This guidance document addresses privacy protections when Americans interact with their government. The guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

The privacy objective of the E-Government Act complements the National Strategy to Secure Cyberspace. As the National Strategy indicates, cyberspace security programs that strengthen protections for privacy and other civil liberties, together with strong privacy policies and practices in the federal agencies, will ensure that information is handled in a manner that maximizes both privacy and security.

Background

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act (see Attachment A). The text of section 208 is provided as Attachment B to this Memorandum. Attachment C provides a general outline of regulatory requirements pursuant to the Children's Online Privacy Protection Act ("COPPA"). Attachment D summarizes the modifications to existing guidance resulting from this Memorandum. A complete list of OMB privacy guidance currently in effect is available at OMB's website.

As OMB has previously communicated to agencies, for purposes of their FY2005 IT budget requests, agencies should submit all required Privacy Impact Assessments no later than October 3, 2003.

For any questions about this guidance, contact Eva Kleederman, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3647, fax (202) 395-5167, e-mail Eva_Kleederman@omb.eop.gov.

Attachments

Attachment A

E-Government Act Section 208 Implementation Guidance

18-F-1517//0954

I. General

A. ***Requirements.*** Agencies are required to:

1. conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available (see Section II of this Guidance),
2. post privacy policies on agency websites used by the public (see Section III),
3. translate privacy policies into a standardized machine-readable format (see Section IV), and
4. report annually to OMB on compliance with section 208 of the E-Government Act of 2002 (see Section VII).

B. ***Application.*** This guidance applies to:

1. all executive branch departments and agencies ("agencies") and their contractors that use information technology or that operate websites for purposes of interacting with the public;
2. relevant cross-agency initiatives, including those that further electronic government.

C.

Modifications to Current Guidance. Where indicated, this Memorandum modifies the following three memoranda, which are replaced by this guidance (see summary of modifications at Attachment D):

1. Memorandum 99-05 (January 7, 1999), directing agencies to examine their procedures for ensuring the privacy of personal information in federal records and to designate a senior official to assume primary responsibility for privacy policy;
2. Memorandum 99-18 (June 2, 1999), concerning posting privacy policies on major entry points to government web sites as well as on any web page collecting substantial personal information from the public; and
3. Memorandum 00-13 (June 22, 2000), concerning (i) the use of tracking technologies such as persistent cookies and (ii) parental consent consistent with the Children's Online Privacy Protection Act ("COPPA").

II. Privacy Impact Assessment

A. ***Definitions.***

1. *Individual* - means a citizen of the United States or an alien lawfully admitted for permanent residence.[1]
2. *Information in identifiable form*- is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).[2]
3. *Information technology (IT)* - means, as defined in the Clinger-Cohen Act[3], any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
4. *Major information system* - embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources.
5. *National Security Systems* - means, as defined in the Clinger-Cohen Act[4], an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.
6. *Privacy Impact Assessment (PIA)*- is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
7. *Privacy policy in standardized machine-readable format*- means a statement about site privacy

18-F-1517//0955

practices written in a standard computer language (not English text) that can be read automatically by a web browser.

B. ***When to conduct a PIA:***[5]

1. *The E-Government Act requires agencies to conduct a PIA before:*
   a. developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
   b. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).
2. *In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:*
   a. Conversions - when converting paper-based records to electronic systems;
   b. Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
   c. Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
      - For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
   d. Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
      - For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.
   e. New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
   f. Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
   g. New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
      - For example the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross agency IT investment.
   h. Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
      - For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.
   i. Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)
3. *No PIA is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged, as in the following circumstances:*
   a. for government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public (this includes government personnel and government contractors and consultants);[6]
   b. for government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or

18-F-1517//0956

obtaining additional information;
c. for national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act);
d. when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act (see 5 U.S.C. §§ 552a(8-10), (e)(12), (o), (p), (q), (r), (u)), which specifically provide privacy protection for matched information;
e. when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the E-Government Act of 2002;
f. if agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generates information in identifiable form;
g. for minor changes to a system or collection that do not create new privacy risks.

4. *Update of PIAs:* Agencies must update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

C. ***Conducting a PIA.***

1. *Content.*
   a. PIAs must analyze and describe:
      i. what information is to be collected (e.g., nature and source);
      ii. why the information is being collected (e.g., to determine eligibility);
      iii. intended use of the information (e.g., to verify existing data);
      iv. with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
      v. what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
      vi. how the information will be secured (e.g., administrative and technological controls[7]); and
      vii. whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.
   b. Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.
2. Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection:
   a. *Specificity.* The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.
      i. *IT development stage.* PIAs conducted at this stage:
         1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
         2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;
         3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.
      ii. *Major information systems.* PIAs conducted for these systems should reflect more extensive analyses of:
         1. the consequences of collection and flow of information,
         2. the alternatives to collection and handling as designed,
         3. the appropriate measures to mitigate risks identified for each alternative and,
         4. the rationale for the final design choice or business process.
      iii. *Routine database systems.* Agencies may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.
   b. *Information life cycle analysis/collaboration.* Agencies must consider the information "life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals' privacy. To be

18-F-1517//0957

comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy.

3. *Review and publication.*
    a. a. Agencies must ensure that:
        i. the PIA document and, if prepared, summary are approved by a "reviewing official" (the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA);
        ii. for each covered IT system for which 2005 funding is requested, and consistent with previous guidance from OMB, the PIA is submitted to the Director of OMB no later than October 3, 2003 (submitted electronically to PIA@omb.eop.gov along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 300[8]); and
        iii. the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).
            1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment[9]. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).
            2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

D. *Relationship to requirements under the Paperwork Reduction Act (PRA)*[10].
1. Joint Information Collection Request (ICR) and PIA. Agencies undertaking new electronic information collections may conduct and submit the PIA to OMB, and make it publicly available, as part of the SF83 Supporting Statement (the request to OMB to approve a new agency information collection).
2. If Agencies submit a Joint ICR and PIA:
    a. All elements of the PIA must be addressed and identifiable within the structure of the Supporting Statement to the ICR, including:
        i. a description of the information to be collected in the response to Item 1 of the Supporting Statement[11];
        ii. a description of how the information will be shared and for what purpose in Item 2 of the Supporting Statement[12];
        iii. a statement detailing the impact the proposed collection will have on privacy in Item 2 of the Supporting Statement[13];
        iv. a discussion in item 10 of the Supporting Statement of:
            1. whether individuals are informed that providing the information is mandatory or voluntary
            2. opportunities to consent, if any, to sharing and submission of information;
            3. how the information will be secured; and
            4. whether a system of records is being created under the Privacy Act)[14].
    b. For additional information on the requirements of an ICR, please consult your agency's organization responsible for PRA compliance.
3. Agencies need not conduct a new PIA for simple renewal requests for information collections under the PRA. As determined by reference to section II.B.2. above, agencies must separately consider the need for a PIA when amending an ICR to collect information that is significantly different in character from the original collection.

E. *Relationship to requirements under the Privacy Act of 1974, 5 U.S. C. 552a.*

1. Agencies may choose to conduct a PIA when developing the System of Records (SOR) notice required by subsection (e)(4) of the Privacy Act, in that the PIA and SOR overlap in content (e.g., the categories of records in the system, the uses of the records, the policies and practices for handling, etc.).
2. Agencies, in addition, may make the PIA publicly available in the Federal Register along with the Privacy Act SOR notice.

18-F-1517//0958

3. Agencies must separately consider the need for a PIA when issuing a change to a SOR notice (e.g., a change in the type or category of record added to the system may warrant a PIA).

III. Privacy Policies on Agency Websites

A. *Privacy Policy Clarification.* To promote clarity to the public, agencies are required to refer to their general web site notices explaining agency information handling practices as the "Privacy Policy."

B. *Effective Date.* Agencies are expected to implement the following changes to their websites by December 15, 2003.

C. *Exclusions:* For purposes of web privacy policies, this guidance does not apply to:
1. information other than "government information" as defined in OMB Circular A-130;
2. agency intranet web sites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees);
3. national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-government Act).

D. *Content of Privacy Policies.*
1. Agency Privacy Policies must comply with guidance issued in OMB Memorandum 99-18 and must now also include the following two new content areas:
   a. *Consent to collection and sharing*[15]. Agencies must now ensure that privacy policies:
      i. inform visitors whenever providing requested information is voluntary;
      ii. inform visitors how to grant consent for use of voluntarily-provided information; and
      iii. inform visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.
   b. *Rights under the Privacy Act or other privacy laws*[16]. Agencies must now also notify web-site visitors of their rights under the Privacy Act or other privacy-protecting laws that may primarily apply to specific agencies (such as the Health Insurance Portability and Accountability Act of 1996, the IRS Restructuring and Reform Act of 1998, or the Family Education Rights and Privacy Act):
      i. in the body of the web privacy policy;
      ii. via link to the applicable agency regulation (e.g., Privacy Act regulation and pertinent system notice); or
      iii. via link to other official summary of statutory rights (such as the summary of Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at www.Firstgov.gov).
2. Agency Privacy Policies must continue to address the following, modified, requirements:
   a. Nature, purpose, use and sharing of information collected . Agencies should follow existing policies (issued in OMB Memorandum 99-18) concerning notice of the nature, purpose, use and sharing of information collected via the Internet, as modified below:
      i. *Privacy Act information.* When agencies collect information subject to the Privacy Act, agencies are directed to explain what portion of the information is maintained and retrieved by name or personal identifier in a Privacy Act system of records and provide a Privacy Act Statement either:
         1. at the point of collection, or
         2. via link to the agency's general Privacy Policy[18].
      ii. *"Privacy Act Statements."* Privacy Act Statements must notify users of the authority for and purpose and use of the collection of information subject to the Privacy Act, whether providing the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.
      iii. *Automatically Collected Information (site management data).* Agency Privacy Policies must specify what information the agency collects automatically (i.e., user's IP address, location, and time of visit) and identify the use for which it is collected (i.e., site management or security purposes).
      iv. *Interaction with children:* Agencies that provide content to children under 13 and that collect personally identifiable information from these visitors should incorporate the requirements of the Children's Online Privacy Protection Act ("COPPA") into their Privacy Policies (see Attachment C)[19].
      v. *Tracking and customization activities.* Agencies are directed to adhere to the following modifications to OMB Memorandum 00-13 and the OMB follow-up guidance letter dated September 5, 2000:
         1. *Tracking technology prohibitions:*

18-F-1517//0959

a. agencies are prohibited from using persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Internet except as provided in subsection (b) below;
b. agency heads may approve, or may authorize the heads of sub-agencies or senior official(s) reporting directly to the agency head to approve, the use of persistent tracking technology for a compelling need. When used, agency's must post clear notice in the agency's privacy policy of:
    - the nature of the information collected;
    - the purpose and use for the information;
    - whether and to whom the information will be disclosed; and
    - the privacy safeguards applied to the information collected.
c. agencies must report the use of persistent tracking technologies as authorized for use by subsection b. above (see section VII)[20].

2. *The following technologies are not prohibited:*
    a. Technology that is used to facilitate a visitor's activity within a single session (e.g., a "session cookie") and does not persist over time is not subject to the prohibition on the use of tracking technology.
    b. Customization technology (to customize a website at the visitor's request) if approved by the agency head or designee for use (see v.1.b above) and where the following is posted in the Agency's Privacy Policy:
        - the purpose of the tracking (i.e., customization of the site);
        - that accepting the customizing feature is voluntary;
        - that declining the feature still permits the individual to use the site; and
        - the privacy safeguards in place for handling the information collected.
    c. Agency use of password access to information that does not involve "persistent cookies" or similar technology.

vi. *Law enforcement and homeland security sharing:* Consistent with current practice, Internet privacy policies may reflect that collected information may be shared and protected as necessary for authorized law enforcement, homeland security and national security activities.

b. *Security of the information*[21]. Agencies should continue to comply with existing requirements for computer security in administering their websites[22] and post the following information in their Privacy Policy:
    i. in clear language, information about management, operational and technical controls ensuring the security and confidentiality of personally identifiable records (e.g., access controls, data storage procedures, periodic testing of safeguards, etc.), and
    ii. in general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems. (The statement should be at a level to inform the public that their information is being protected while not compromising security.)

E. *Placement of notices.* Agencies should continue to follow the policy identified in OMB Memorandum 99-18 regarding the posting of privacy policies on their websites. Specifically, agencies must post (or link to) privacy policies at:
    1. their principal web site;
    2. any known, major entry points to their sites;
    3. any web page that collects substantial information in identifiable form.
F. ***Clarity of notices.*** Consistent with OMB Memorandum 99-18, privacy policies must be:
    1. clearly labeled and easily accessed;
    2. written in plain language; and
    3. made clear and easy to understand, whether by integrating all information and statements into a single posting, by layering a short "highlights" notice linked to full explanation, or by other means the agency determines is effective.

IV. Privacy Policies in Machine-Readable Formats

A. ***Actions.***
    1. Agencies must adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make

18-F-1517//0960

an informed choice about whether to conduct business with that site.
2. OMB encourages agencies to adopt other privacy protective tools that become available as the technology advances.

B. ***Reporting Requirement.*** Agencies must develop a timetable for translating their privacy policies into a standardized machine-readable format. The timetable must include achievable milestones that show the agency's progress toward implementation over the next year. Agencies must include this timetable in their reports to OMB (see Section VII).

V. Privacy Policies Incorporated by this Guidance

In addition to the particular actions discussed above, this guidance reiterates general directives from previous OMB Memoranda regarding the privacy of personal information in federal records and collected on federal web sites. Specifically, existing policies continue to require that agencies:

A. assure that their uses of new information technologies sustain, and do not erode, the protections provided in all statutes relating to agency use, collection, and disclosure of personal information;
B. assure that personal information contained in Privacy Act systems of records be handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
C. evaluate legislative proposals involving collection, use and disclosure of personal information by the federal government for consistency with the Privacy Act of 1974;
D. evaluate legislative proposals involving the collection, use and disclosure of personal information by any entity, public or private, for consistency with the Privacy Principles;
E. ensure full adherence with stated privacy policies.

VI. Agency Privacy Activities/Designation of Responsible Official

Because of the capability of information technology to capture and disseminate information in an instant, all federal employees and contractors must remain mindful of privacy and their obligation to protect information in identifiable form. In addition, implementing the privacy provisions of the E-Government Act requires the cooperation and coordination of privacy, security, FOIA/Privacy Act and project officers located in disparate organizations within agencies. Clear leadership and authority are essential.

Accordingly, this guidance builds on policy introduced in Memorandum 99-05 in the following ways:

A. Agencies must:
   1. inform and educate employees and contractors of their responsibility for protecting information in identifiable form;
   2. identify those individuals in the agency (e.g., information technology personnel, Privacy Act Officers) that have day-to-day responsibility for implementing section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies.
   3. designate an appropriate senior official or officials (e.g., CIO, Assistant Secretary) to serve as the agency's principal contact(s) for information technology/web matters and for privacy policies. The designated official(s) shall coordinate implementation of OMB web and privacy policy and guidance.
   4. designate an appropriate official (or officials, as appropriate) to serve as the "reviewing official(s)" for agency PIAs.

B. OMB leads a committee of key officials involved in privacy that reviewed and helped shape this guidance and that will review and help shape any follow-on privacy and web-privacy-related guidance. In addition, as part of overseeing agencies' implementation of section 208, OMB will rely on the CIO Council to collect information on agencies' initial experience in preparing PIAs, to share experiences, ideas, and promising practices as well as identify any needed revisions to OMB's guidance on PIAs.

VII. Reporting Requirements

Agencies are required to submit an annual report on compliance with this guidance to OMB as part of their annual E-Government Act status report. The first reports are due to OMB by December 15, 2003. All agencies that use information technology systems and conduct electronic information collection activities must complete a report on compliance with this guidance, whether or not they submit budgets to OMB.

Reports must address the following four elements:

A. *Information technology systems or information collections for which PIAs were conducted.* Include the mechanism by which the PIA was made publicly available (website, Federal Register, other), whether the PIA was made publicly available in full, summary form or not at all (if in summary form or not at all, explain), and, if made available in conjunction with an ICR or SOR, the publication date.
B. *Persistent tracking technology uses.* If persistent tracking technology is authorized, include the need that

18-F-1517//0961

compels use of the technology, the safeguards instituted to protect the information collected, the agency official approving use of the tracking technology, and the actual privacy policy notification of such use.

C. *Agency achievement of goals for machine readability*: Include goals for and progress toward achieving compatibility of privacy policies with machine-readable privacy protection technology.

D. *Contact information*. Include the individual(s) (name and title) appointed by the head of the Executive Department or agency to serve as the agency's principal contact(s) for information technology/web matters and the individual (name and title) primarily responsible for privacy policies.

Attachment B
E-Government Act of 2002
Pub. L. No. 107-347, Dec. 17, 2002

SEC. 208. PRIVACY PROVISIONS.

A. PURPOSE. — The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

B. PRIVACY IMPACT ASSESSMENTS.—

1. RESPONSIBILITIES OF AGENCIES.—
    a. IN GENERAL.—An agency shall take actions described under subparagraph (b) before—
        i. developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
        ii. initiating a new collection of information that—
            1. will be collected, maintained, or disseminated using information technology; and
            2. includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.
    b. AGENCY ACTIVITIES. —To the extent required under subparagraph (a), each agency shall—
        i. conduct a privacy impact assessment;
        ii. ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and
        iii. if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.
    c. SENSITIVE INFORMATION. —Subparagraph (b)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.
    d. COPY TO DIRECTOR. —Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.
2. CONTENTS OF A PRIVACY IMPACT ASSESSMENT. —
    a. IN GENERAL. —The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.
    b. GUIDANCE. — The guidance shall—
        i. ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and
        ii. require that a privacy impact assessment address—
            1. what information is to be collected;
            2. why the information is being collected;
            3. the intended use of the agency of the information;
            4. with whom the information will be shared;
            5. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
            6. how the information will be secured; and
            7. whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the `Privacy Act').
3. RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—
    a. develop policies and guidelines for agencies on the conduct of privacy impact assessments;
    b. oversee the implementation of the privacy impact assessment process throughout the Government; and
    c. require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

18-F-1517//0962

C. PRIVACY PROTECTIONS ON AGENCY WEBSITES. —

1. PRIVACY POLICIES ON WEBSITES. —
    a. GUIDELINES FOR NOTICES. —The Director shall develop guidance for privacy notices on agency websites used by the public.
    b. CONTENTS. —The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—
        i. what information is to be collected;
        ii. why the information is being collected;
        iii. the intended use of the agency of the information;
        iv. with whom the information will be shared;
        v. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
        vi. how the information will be secured; and
        vii. the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the `Privacy Act'), and other laws relevant to the protection of the privacy of an individual.
2. PRIVACY POLICIES IN MACHINE-READABLE FORMATS. — The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

D. DEFINITION. —In this section, the term `identifiable form' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Attachment C

This attachment is a summary by the Federal Trade Commission of its guidance regarding federal agency compliance with the Children's Online Privacy Protection Act (COPPA).

The hallmarks of COPPA for purposes of federal online activity are (i) notice of information collection practices (ii) verifiable parental consent and (iii) access, as generally outlined below:

- Notice of Information Collection Practices

  Agencies whose Internet sites offer a separate children's area and collect personal information from them must post a clear and prominent link to its Internet privacy policy on the home page of the children's area and at each area where it collects personal information from children. The privacy policy should provide the name and contact information of the agency representative required to respond to parental inquiries about the site. Importantly, the privacy policy should inform parents about the kinds of information collected from children, how the information is collected (directly, or through cookies), how the information is used, and procedures for reviewing/deleting the information obtained from children.

  In addition, the privacy policy should inform parents that only the minimum information necessary for participation in the activity is collected from the child.In addition to providing notice by posting a privacy policy, notice of an Internet site's information collection practices must be sent directly to a parent when a site is requesting parental consent to collection personal information from a child. This direct notice should tell parents that the site would like to collect personal information from their child, that their consent is required for this collection, and how consent can be provided. The notice should also contain the information set forth in the site's privacy policy, or provide an explanatory link to the privacy policy.

- Verifiable Parental Consent

  With limited exceptions, agencies must obtain parental consent before collecting any personal information from children under the age of 13. If agencies are using the personal information for their internal use only, they may obtain parental consent through an e-mail message from the parent, as long as they take additional steps to increase the likelihood that the parent has, in fact, provided the consent. For example, agencies might seek confirmation from a parent in a delayed confirmatory e-mail, or confirm the parent's consent by letter or phone call[23].

  However, if agencies disclose the personal information to third parties or the public (through chat rooms or message boards), only the most reliable methods of obtaining consent must be used. These methods include: (i) obtaining a signed form from the parent via postal mail or facsimile, (ii) accepting and verifying a credit card number in connection with a transaction, (iii) taking calls from parents through a toll-free telephone

18-F-1517//0963

number staffed by trained personnel, or (iv) email accompanied by digital signature.

Although COPPA anticipates that private sector Internet operators may share collected information with third parties (for marketing or other commercial purposes) and with the public (through chat rooms or message boards), as a general principle, federal agencies collect information from children only for purposes of the immediate online activity or other, disclosed, internal agency use. (Internal agency use of collected information would include release to others who use it solely to provide support for the internal operations of the site or service, including technical support and order fulfillment.) By analogy to COPPA and consistent with the Privacy Act, agencies may not use information collected from children in any manner not initially disclosed and for which explicit parental consent has not been obtained. Agencies' Internet privacy policies should reflect these disclosure and consent principles.

COPPA's implementing regulations include several exceptions to the requirement to obtain advance parental consent where the Internet operator (here, the agency) collects a child's email address for the following purposes: (i) to provide notice and seek consent, (ii) to respond to a one-time request from a child before deleting it, (iii) to respond more than once to a specific request, e.g., for a subscription to a newsletter, as long as the parent is notified of, and has the opportunity to terminate a continuing series of communications, (iv) to protect the safety of a child, so long as the parent is notified and given the opportunity to prevent further use of the information, and (v) to protect the security or liability of the site or to respond to law enforcement if necessary.

Agencies should send a new notice and request for consent to parents any time the agency makes material changes in the collection or use of information to which the parent had previously agreed. Agencies should also make clear to parents that they may revoke their consent, refuse to allow further use or collection of the child's personal information and direct the agency to delete the information at any time.

- Access

At a parent's request, agencies must disclose the general kinds of personal information they collect online from children as well as the specific information collected from a child. Agencies must use reasonable procedures to ensure they are dealing with the child's parent before they provide access to the child's specific information, e.g., obtaining signed hard copy of identification, accepting and verifying a credit card number, taking calls from parents on a toll-free line staffed by trained personnel, email accompanied by digital signature, or email accompanied by a PIN or password obtained through one of the verification methods above.

In adapting the provisions of COPPA to their Internet operations, agencies should consult the FTC's web site at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html or call the COPPA compliance telephone line at (202) 326-3140.

Attachment D

Summary of Modifications to Prior Guidance

This Memorandum modifies prior guidance in the following ways:

* Internet Privacy Policies (Memorandum 99-18):

- must identify when tracking technology is used to personalize the interaction, and explain the purpose of the feature and the visitor's option to decline it.

- must clearly explain when information is maintained and retrieved by personal identifier in a Privacy Act system of records; must provide (or link to) a Privacy Act statement (which may be subsumed within agency's Internet privacy policy) where Privacy Act information is solicited.

- should clearly explain an individual's rights under the Privacy Act if solicited information is to be maintained in a Privacy Act system of records; information about rights under the Privacy Act may be provided in the body of the web privacy policy or via link to the agency's published systems notice and Privacy Act regulation or other summary of rights under the Privacy Act (notice and explanation of rights under other privacy laws should be handled in the same manner).

- when a Privacy Act Statement is not required, must link to the agency's Internet privacy policy explaining the purpose of the collection and use of the information (point-of-collection notice at agency option).

18-F-1517//0964

- must clearly explain where the user may consent to the collection or sharing of information and must notify users of any available mechanism to grant consent.
- agencies must undertake to make their Internet privacy policies "readable" by privacy protection technology and report to OMB their progress in that effort.
- must adhere to the regulatory requirements of the Children's Online Privacy Protection Act (COPPA) when collecting information electronically from children under age 13.

*Tracking Technology (Memorandum 00-13):

- prohibition against tracking visitors' Internet use extended to include tracking by any means (previous guidance addressed only "persistent cookies").? authority to waive the prohibition on tracking in appropriate circumstances may be retained by the head of an agency, or may be delegated to (i) senior official(s) reporting directly to the agency head, or to (ii) the heads of sub-agencies.? agencies must report the use of tracking technology to OMB, identifying the circumstances, safeguards and approving official.
- agencies using customizing technology must explain the use, voluntary nature of and the safeguards applicable to the customizing device in the Internet privacy policy.
- agency heads or their designees may approve the use of persistent tracking technology to customize Internet interactions with the government.

* Privacy responsibilities (Memorandum 99-05)

- agencies to identify individuals with day-to-day responsibility for implementing the privacy provisions of the E-Government Act, the Privacy Act and any other applicable statutory privacy regime.
- agencies to report to OMB the identities of senior official(s) primarily responsible for implementing and coordinating information technology/web policies and privacy policies.

---

1. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.
2. Information in identifiable form is defined in section 208(d) of the Act as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Information "permitting the physical or online contacting of a specific individual" (see section 208(b)(1)(A)(ii)(II)) is the same as "information in identifiable form."
3. Clinger-Cohen Act of 1996, 40 U.S.C. 11101(6).
4. Clinger-Cohen Act of 1996, 40 U.S.C. 11103.
5. In addition to these statutorily prescribed activities, the E-Government Act authorizes the Director of OMB to require agencies to conduct PIAs of existing electronic information systems or ongoing collections of information in identifiable form as the Director determines appropriate. (see section 208(b)(3)(C)).
6. Information in identifiable form about government personnel generally is protected by the Privacy Act of 1974. Nevertheless, OMB encourages agencies to conduct PIAs for these systems as appropriate.
7. Consistent with agency requirements under the Federal Information Security Management Act, agencies should: (i) affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured, (ii) acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls, (iii) describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information, and (iv) provide a point of contact for any additional questions from users. Given the potential sensitivity of security-related information, agencies should ensure that the IT security official responsible for the security of the system and its information reviews the language before it is posted.
8. PIAs that comply with the statutory requirements and previous versions of this Memorandum are acceptable for agencies' FY 2005 budget submissions.
9. Section 208(b)(1)(C).
10. See 44 USC Chapter 35 and implementing regulations, 5 CFR Part 1320.8.
11. Item 1 of the Supporting Statement reads: "Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information."
12. Item 2 of the Supporting Statement reads: "Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information

18-F-1517//0965

received from the current collection."

13. Item 2 of the Supporting Statement reads: "Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection."
14. Item 10 of the Supporting Statement reads: "Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy."
15. Section 208(c)(1)(B)(v).
16. Section 208(c)(1)(B)(vii).
17. Section 208(c)(1)(B)(i-iv).
18. When multiple Privacy Act Statements are incorporated in a web privacy policy, a point-of-collection link must connect to the Privacy Act Statement pertinent to the particular collection.
19. Attachment C contains a general outline of COPPA's regulatory requirements. Agencies should consult the Federal Trade Commission's COPPA compliance telephone line at (202)-326-3140 or website for additional information at: http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.
20. Consistent with current practice, the agency head or designee may limit, as appropriate, notice and reporting of tracking activities that the agency has properly approved and which are used for authorized law enforcement, national security and/or homeland security purposes.
21. Section 208(c)(1)(B)(vi).
22. Federal Information Security Management Act of 2002 (Title III of P.L. 107-347), OMB's related security guidance and policies (Appendix III to OMB Circular A-130, "Security of Federal Automated Information Resources") and standards and guidelines development by the National Institute of Standards and Technologies.
23. This standard was set to expire in April 2002, at which time the most verifiable methods of obtaining consent would have been required; however, in a Notice of Proposed Rulemaking, published in the Federal Register on October 31, 2001, the FTC has proposed that this standard be extended until April 2004. 66 Fed. Reg. 54963.

18-F-1517//0966

Exhibit 6

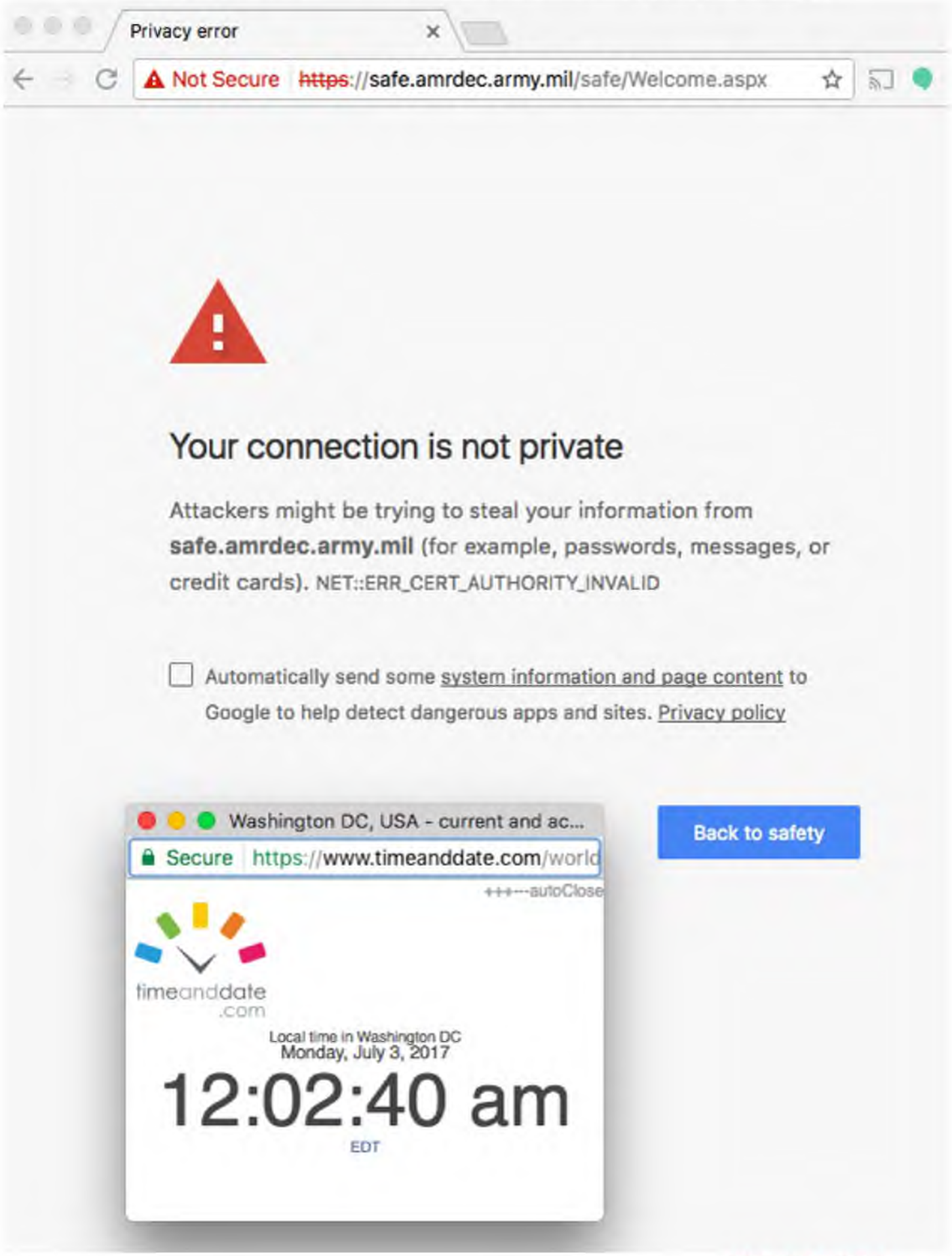

Privacy error
Not Secure https://safe.amrdec.army.mil/safe/Welcome.aspx
Your connection is not private
Attackers might be trying to steal your information from safe.amrdec.army.mil (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID
Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy
Back to safety
Washington DC, USA - current and ac...
Secure https://www.timeanddate.com/world
timeanddate.com
Local time in Washington DC
Monday, July 3, 2017
12:02:40 am
EDT

Exhibit 7

DECLARATION OF NAME

I, Kimberly Bryant, declare as follows:

1. My name is Kimberly Bryant. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident San Francisco, CA.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in California.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed July 5, 2017

Kimberly Bryant
NAME

Exhibit 8

DECLARATION OF Julie E. Cohen

I, Julie E. Cohen, declare as follows:

1. My name is Julie E. Cohen. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident of Bethesda, MARYLAND.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in MARYLAND.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed July 5, 2017

Julie E. Cohen

Exhibit 9

DECLARATION OF William T. Coleman III

I, William T. Coleman III, declare as follows:

1. My name is William T. Coleman III. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident Los Altos, California.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in Los Altos, California.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed July 5, 2017

William T. Coleman III

Exhibit 10

DECLARATION OF Harry R. Lewis

I, Harry R. Lewis, declare as follows:

1. My name is Harry R. Lewis. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident Brookline, Massachusetts.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in Massachusetts.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed July 5, 2017

Harry R. Lewis

Exhibit 11

DECLARATION OF PABLO GARCIA MOLINA

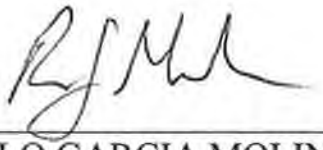
I, **PABLO GARCIA MOLINA**, declare as follows:

1. My name is **PABLO GARCIA MOLINA**. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident of WASHINGTON, DC.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in DC.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed July 5, 2017



PABLO GARCIA MOLINA

Exhibit 12

DECLARATION OF NAME (Peter G Neumann)

I, Peter G. Neumann declare as follows:

1. My name is Peter G. Neumann. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident Palo Alto, California.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in California.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed July 5, 2017

Peter G Neumann

Peter G Neumann 7/5/2017

Exhibit 13

DECLARATION OF BRUCE SCHNEIER

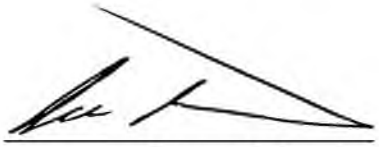
I, Bruce Schneier, declare as follows:

1. My name is Bruce Schneier. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident of Minneapolis, Minnesota.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in Minnesota.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed July 5, 2017



Bruce Schneier

Exhibit 14

DECLARATION OF James Waldo

I, James Waldo, declare as follows:

1. My name is James Waldo. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident Dracut, Massachusetts.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in Massachusetts.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed July 5, 2017

James Waldo

Exhibit 15

DECLARATION OF Shoshana Zuboff

I, Shoshana Zuboff, declare as follows:

1. My name is Shoshana Zuboff. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident Nobleboro, Maine.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in Maine.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed July 5, 2017

Shoshana Zuboff

Shoshana Zuboff

Exhibit 16

NCSL
THE CANVASS
STATES AND ELECTION REFORM®

Issue 66 | February 2016

CANVASS (n.)

Compilation of election returns and validation of the outcome that forms the basis of the official results by a political subdivision.

—U.S. Election Assistance Commission: Glossary of Key Election Terminology

It's a Presidential Election Year: Do You Know Where Your Voter Records Are?

One of the secrets of the election world is how readily available voter data can be—and it's been making headlines lately. In late 2015, information such as name, address, party, and voting history relating to approximately 191 million voters was published online. And recently, the presidential campaign of Texas Senator Ted Cruz came under fire for a mailer in Iowa that used voter data to assign grades to voters and compared them to neighbors to motivate turnout. Voter records have always been public information, but now it's being used in new ways. Here are some key facts you need to know about the privacy (or lack of privacy) of voter information.

What voter information is public record?

All 50 states and the District of Columbia provide access to voter information, according to the U.S. Elections Project run by Dr. Michael McDonald at the University of Florida; but as with everything related to elections there are 51 different variations on what information is provided, who can access it, and how much it costs to get it.

Generally, all states provide the name and address of the registered voter. From there it gets complicated. Some states have statutory limitations on what information is available. At least 25 states limit access to social security numbers, date of birth or other identifying factors such as a driver's license number. Ten states limit the contact information, such as a telephone number or email address. Nine states include miscellaneous information like place of birth, voter identification numbers, race, gender, secondary addresses, accommodations to vote and signatures on the list of exemptions for the voter file. Texas specifically restricts the residential address of any judge in the state.

While, there are 13 states that have no codified restrictions on the information available to the public, the secretary of state may have the ability to limit information. Six states have a general prohibition on "information of a personal nature" or information related to matters of individual safety that pertain to voter records as well as all other state records.

Every state except Rhode Island as well as the District of Columbia also provide information about voter history —not who a person voted for but just if they voted (Rhode Island does not provide access to that information). Absentee voting information—ballot requests or permanent absentee lists—are also available, sometimes for an extra fee and sometimes only through municipalities or local jurisdictions. At least five states do not offer absentee voting data as part of the available voter file.

(cont. on page 2)

Inside this Issue

TO SUBSCRIBE to *The Canvass*, please email a request to TheCanvass@ncsl.org

(Voter Records, cont. from page 1)

Who can access the information?

All states allow candidates for elected offices or political parties to access voter records, typically for political purposes. Which makes sense—if you want to run for office it helps to have a list of your constituents to contact.

Beyond candidates and political parties, who can access voter lists varies state by state. Eleven states do not allow members of the public to access voter data. Several other states restrict access to state residents (11), other registered voters (7), non-profit organizations (6), and those doing research (9).

What can it be used for?

Most often, voter information can be used for "non-commercial" purposes only—in other words, an entity or person can't access the information to sell a product or a service, but can use it for anything else.

Several states are stricter, limiting the use to just political purposes or election purposes, which may or may not include voter registration drives, getting-out-the-vote and research. Further, the available uses may vary between the different users groups mentioned above. And it can be hard for states to control what happens to the data once it's been turned over.

Cost for accessing data

Accessing voter data comes with a price. "There is a wide variation in the costs that states charge for accessing this information," says McDonald.

Washington, D.C. only charges $2 for the entire voter registration list; other bargain rates include Arkansas ($2.50) and New Jersey ($2.55).

In Massachusetts, New York , Ohio, Oklahoma, Vermont, Washington or Wyoming accessing the voter is free, provided you meet the criteria.

Accessing the date is much pricier in some states. Several states charge $5,000 and Wisconsin charges $12,500. Alabama and Arizona got creative with setting their fees by charging one cent per voter, resulting in a cost of upwards of $30,000.

Ultimately, the average cost for a voter list is approximately $1,825—which isn't prohibitively expensive.

What other exceptions are there?

As mentioned above, states can restrict certain information from being released in the voter file. But states can also withhold information if a voter's information is marked as confidential.

Thirty-nine states maintain address confidentiality programs designed to keep the addresses of victims of domestic violence or abuse, sexual assault or stalking out of public records for their protection. The programs allow victims to use an alternate address, usually a government post office box, in place of their actual home address. Of those 39 states, at least 29 of them have specific references to voter registration and voter records. That means those voter records won't be included in the comprehensive list purchased from the state.

In 2015, Iowa established an address confidentiality program that includes voter records and Florida updated their address confidentiality law to include victims of stalking. This year Kentucky and New York have legislation to connect address confidentiality to voter records.

Another sensitive demographic is 16- and 17 year-olds that may be able to preregister under state law. How do you protect the information of minors? Of course the answer is complicated. Utah considers the records of preregistered voters private under

(cont. on page 3)

Voter-Shaming—How does Social Pressure Influence Voter Turnout?

Get ready to add "voter-shaming" to your vocabulary. The term has been popping up in news stories everywhere over the past month—most notably in controversial presidential campaign mail pieces that compared the voting history of Iowa voters to their neighbors. But just what is it exactly?

The practice of comparing voting history to that of peers stems from a 2008 study conducted by Alan Gerber and Donald Green from Yale University and Christopher Larimer from the University of Northern Iowa entitled Social Pressure and Voter Turnout: Evidence from a Large Scale Field Experiment.

The study examined the effect of various mailings on voter turnout. Specifically, the mailers had different messages that encouraged voters to do their civic duty, indicated that the voter's vote history was being studied, listed the vote history of each member of the household, or listed the voter's vote history compared to their neighbors. The results showed that each of these "social pressures" increased voter turnout but none more so than the neighbor mailing which increased turnout by eight percent.

Candidates, campaigns and other researchers took notice of the study which has resulted in "voter-shaming" mailers popping up in places like Alaska, North Carolina and most recently in the first two presidential nominating contests in the nation—Iowa and New Hampshire. They've shown to be powerful motivators so keep an eye out for social pressure mailers coming soon to your mailbox.

18-F-1517//0998

(Voter Records, cont. from page 2)

state law and Minnesota designates preregistered voters as "pending" until they become eligible in which case they are changed to "active." Only active voters are included on the public voter list. The same is true in Louisiana, Missouri, New Jersey and Rhode Island.

In states where 17-year-olds are on the active voter rolls because they'll be able to vote in the next election, their information will be treated like all the other voters. That's the case in Nebraska where 17-year-olds can register, and in some cases vote, if they turn 18 by the first Tuesday after the first Monday in November. Maine doesn't allow the public to access the voter list, but since the Pine Tree State allows 17-year-olds who will be 18 by the general election to vote in primaries, that information is included on the lists accessible to candidates and political parties. Delaware, Iowa, Nevada and Oregon have similar systems in which those under 18 are included on the list if they turn 18 by the date of the general election or are eligible to vote in primaries. Florida includes the information of preregistered voters unless an exemption is claimed.

How have legislatures responded?

Sen. Paul Doyle (CT)

In 2015, 16 bills in 12 states were introduced that dealt with some aspect of distribution and the availability of voter information . In Connecticut, Senator Paul Doyle (D) responded to constituent concerns about their voter information being publicly available online by filing legislation to specifically prohibit that information from being published on the Internet. "My constituent told me that they were going to take themselves off the voter list and de-register because of their information being available online—that's a problem," says Doyle. "I understand First Amendment concerns, but I wanted to start the discussion on the issue."

Three bills were enacted in 2015. In addition to the Florida and Iowa bills mentioned above, Alabama decided to allow state legislators to receive only one free copy of the voter list for their district rather than two.

So far in 2016, there are 13 bills in 8 states—some carried over from last year—dealing with voter information and a few those are carryovers from 2015. One of the more notable battles is being waged in Florida where Senator Thad Altman (R) has introduced legislation to make voters' residential addresses, dates of birth, telephone numbers and email addresses confidential and only available to candidates, political parties and election officials, and not to the public. Senator Altman's bill also seeks to protect all the personal information of 16-and 17-year-olds who preregister to vote. The bill has the support of the Florida State Association of Supervisors of Elections.

Sen. Thad Altman (FL)

"Right now all this data is public information," says Altman. "You can put it on the Internet or resell it. You can see someone's address, phone number, and party affiliation. There have been cases where someone received an electioneering piece that said how many times they voted. I'm concerned it could keep people from voting or registering to vote or lead to discrimination. If you want that information to be private you should have that right."

Other states are tackling this issue as well. West Virginia is considering legislation to keep private the address of law enforcement officers and their families. Massachusetts is one of the states that offers voter information for free, but now has legislation to limit public access and to charge for lists. Legislation in Kentucky seeks to remove social security numbers from the voter list. Lastly, Illinois wants to make sure you know who paid for voter information on any mailings that use your voter history.

But there are some who are concerned states may go too far in limiting access to this information. "I'm a researcher who studies voting trends to improve elections—I need access to this information," says McDonald. "There has to be a balance between privacy concerns and access."

Given some of the recent headlines, it remains to be seen how states will react to the increased concern of voter privacy. It's the information age where answers are available at the click of a button and that includes voter information.

One big number

144 million

144 million. The approximate number of eligible American voters that did not vote in the 2014 elections according to data from the U.S. Elections Project and quoted by The Pew Charitable Trusts' David Becker in the Stanford Social Innovation Review. It's one of a 15-part series called "Increasing Voter Turnout: It's Tougher Than You Think."

Becker calls for a two part approach. First—conduct research; more specifically "comprehensive surveys of the eligible electorate that never or rarely votes to assess the attitudes and behaviors of these potential voters." Then "create field experiments that test the effectiveness of various messages and modes of contact on nonvoters, maintaining a randomized control group that would receive no encouragement to vote." The end result could be a "toolkit for those seeking to engage citizens in the democratic process to reach potential voters in a highly efficient, cost-effective way."

18-F-1517//0999

Election Legislation By the Numbers: 2015 and 2016

Election years are notoriously stodgy when it comes to enacting election legislation. First, a recap of 2015:

- 2,355 election-related bills were introduced.
- 241 bills in 45 states were enacted.
- 17 bills in seven states were vetoed.

Highlights included online voter registration, automatic voter registration and items related to preparing for the presidential election. For more information on what exactly was enacted in each states visit NCSL's 2015 Elections Legislation Enacted by State Legislatures webpage.

Now onto 2016:

- 1,747 election-related bills have been introduced in 42 states, including some bills from 2015 that were carried-over into 2016.
- Ten bills have been enacted already including: one in Michigan that eliminates straight-ticket voting; one in New Hampshire that allows local selectman to appoint a replacement if they can't fulfill their duties on election; four in New Jersey, which allow preregistration for 17-year- olds, standardize polling place hours and deal with other administrative issues; two in South Dakota including authorizing the use of vote centers and electronic pollbooks statewide; and one in West Virginia concerning candidate withdrawal from the ballot.
- Automatic voter registration seems to be leading the pack this year with a big increase in legislation from 2015. So far in 2016, 88 bills in 27 states have been introduced which is a 25 percent increase from last year.

- Voter ID legislation continues to be common, with 74 bills introduced so far and Missouri poised to join the ranks of strict voter ID states.
- Absentee voting issues remains popular with 68 bills pending and several states looking at early voting or no-excuse absentee voting.
- Because online voter registration is now active or authorized in 32 states plus the District of Columbia, legislation on this has taken an expected dip. Only 16 bills are in the hopper, but with high profile states like Ohio and Wisconsin considering enacting systems, online voter registration will remain a hot topic.
- Other registration issues, like preregistration for youth, same day registration and list maintenance, are still hot topics with a combined 129 bills.
- 179 bills deal with poll workers, polling places and vote centers.
- 134 bills deal with some aspect of the primary process.
- Voting equipment and technology bills total 53.
- 68 bills address election crimes.

NCSL's Elections Legislation Database is your go-to resource for all things 2016 election legislation. Stay tuned for updates throughout the year.

How many states allow a candidate to withdraw from the ballot after already qualifying?

All but six states allow candidates to withdraw after making it onto the ballot. This is generally subject to some exceptions, most often deadlines after which a candidate may not withdraw. These deadlines are usually well in advance of the election, but in some states the deadline is much closer to the election. For example, in Alabama a candidate may withdraw even after ballots have been printed for the election. In Arizona, Georgia, Hawaii, Maine, Ohio, and Wyoming candidates may withdraw after ballots have been printed, but election officials must post notice of the withdrawal in prominent locations in polling places. Only California, Kansas, New Hampshire, and Wisconsin expressly prohibit candidates from withdrawing from the ballot. Utah and Tennessee do not specifically address candidate withdrawal in statute. In Kansas the rule isn't absolute: A candidate may withdraw from the ballot if they certify to the Secretary of State that they do not reside in Kansas. In New Hampshire, a candidate may not withdraw once they have received a nomination, but they may be disqualified for age, health, or residency reasons. In Wisconsin, the name of a candidate may be removed from the ballot only if the candidate dies before the election, although a candidate may refuse to take office after being elected. For the full list contact the elections team.

18-F-1517//1000

From the Chair

Assembly Member Sebastian Ridley-Thomas serves as chairman of the Elections and Redistricting Committee in the California Assembly. He represents the 54th Assembly district which is entirely in Los Angeles County and consists of communities in the western part of the city of Los Angeles. Assembly Member Ridley-Thomas spoke to The Canvass on Feb. 24.

Assembly Member Sebastian Ridley-Thomas

- "We've done a great deal on language access, accessibility for those with special needs and engaging our high school students and young people through preregistration and other means. The new motor voter law will help to add potentially 5 million people to the voter rolls, but now they have to turn out to vote."
- "We are working with several groups on legislation to give special districts more flexibility in transitioning from at-large representation to district-based representation (AB 2389). Currently, these special districts can only make this change after receiving approval from the voters. Enabling them to do it by ordinance will save time and money, especially in court costs, and help to de-escalate the tension in the courts. The residents will be better represented through this method. Communities are better served when they can elevate members of their own choosing that reflect them and their priorities."
- "Myself and Senator Ben Allen (chair of the Senate Committee on Elections and Constitutional Amendments) are among the youngest legislators and we are focused on the future, but also not leaving our peers behind. I'm proud that California is looking toward the future and making elections better and more collaborative so voters can express their will and values at the ballot box. California is the innovation hub of the world and there's no reason that can't apply to elections."

Read the full interview with Assembly Member Ridley-Thomas.

The Election Administrator's Perspective

Sue Ganje serves as the auditor for Fall River County and Oglala Lakota County (formerly Shannon County) in southwest South Dakota. She is one of two auditors in South Dakota that cover multiple counties; Oglala Lakota County doesn't have a county seat, so the administrative offices are in Fall River County. Ganje spoke to The Canvass on Feb. 18.

Fall River County/Oglala Lakota County Auditor Sue Ganje

- "Things have definitely changed. I can remember hand-counting ballots into the early morning hours and using different colored ballots and straight party voting for political parties. When I look at where we were then to where we are now—we've come a long way in elections."
- "I'm very interested in vote centers. Everywhere you go is a distance in our counties. There can be 30, 40 or sometimes 50 miles between towns. If a voter is not at the right location for voting at the time the polls close, they may have to vote a provisional ballot that may or not be counted. Vote centers would help alleviate that problem. Right now, the county cannot afford the equipment needed for a vote center but I hope there will be funding in the future."
- "I'm proud that we've helped every voter we can to cast a vote. We have a great statewide voter registration system in South Dakota. It's very easy for us to use and we have all the relevant county records right there in order to update the voter records. I think other states should be looking at our system to use."
- "I think we also have a good voter identification system. The state created a personal identification affidavit that voters who do not have IDs can sign at the polls. It works well, and the voter can then vote a regular ballot, not a provisional one. The worst thing we want to do as election officials is turn someone away from the polls. Everyone gets to vote here."

Read the full interview with Ganje.

18-F-1517//1001

Worth Noting

- The Maryland Legislature has overridden the veto of Governor Larry Hogan and will now restore voting rights to felons once they have completed their prison sentence. Previously felons waited until completing parole and probation to get voting rights restored.
- Voter ID is back in the news as the Missouri Senate considers two measures to require voter identification. One is a constitutional amendment that would be sent to voters for their approval and the other would limit the types of identification that can be used. Both measures previously passed the Missouri House.
- Speaking of voter ID, NPR has a look at the issue along with the recent changes made to the state instructions on the federal voter registration form by the U.S. Election Assistance Commission (EAC).
- Politico has an excellent piece on how the recent passing of Supreme Court Justice Antonin Scalia could affect cases and court rulings related to elections and redistricting.
- The plan by the Virginia Republican Party to require loyalty oaths for voters in the Republican Presidential Primary has been scrapped after earning the ire of presidential candidate Donald Trump and others. The Old Dominion State has an open primary that lets independents participate.
- As online voter registration continues to gain steam in states, David Levine, an election management consultant, offers five key steps to getting online voter registration right in electionlineWeekly.
- Oregon, the first state in the country to have automatic voter registration, began implementing its program in January. The Beaver State has added 4,653 voters to the rolls since the law took effect.
- Nebraska is the latest state grappling with legislation allowing voters to take ballot selfies.
- A new year means a new look at why Americans aren't yet voting over the Internet or on their phones according to USA Today.
- New Mexico is on the cusp of allowing 17-year-olds to participate in primary elections if they will turn 18 by the general election.
- The uncertainty surrounding the boundaries for two North Carolina congressional districts may have an impact on military and absentee voters who have already begun early voting for the March primary.
- Straight-ticket voting could be as dead as the dodo in a few years—one of the few remaining states to allow the practice, Indiana, is looking at eliminating it.
- The Election Law Program at William and Mary Law School has a series of helpful video modules on various election issues, like campaign finance, public access to voted ballots, voting equipment malfunctions and absentee ballot disputes.

Replacing outdated voting machines is one of the hottest topics in election news right now so keep an eye on NCSL's Election Technology News Feed for all the latest on election technology and funding from around the nation. The page collects news articles on purchases, and discussions about voting systems, electronic pollbooks or other major decisions, broken down by state.

The NCSL team has been hard at work updating several of our webpages to provide the most current information: 2016 State Primary Dates, Online Voter Registration, Voter ID, Absentee and Early Voting, and Provisional Ballots.

Thanks for reading, let us know your news and please stay in touch.

*—**Wendy Underhill and Dan Diorio***

The Canvass, an Elections Newsletter for Legislatures © 2015
Published by the National Conference of State Legislatures
William T. Pound, Executive Director

In conjunction with NCSL, funding support for *The Canvass* is provided by The Pew Charitable Trusts' Election Initiatives project.

Any opinions, findings or conclusions in this publication are those of NCSL and do not necessarily reflect the views of The Pew Charitable Trusts. Links provided do not indicate NCSL or The Pew Charitable Trusts endorsement of these sites.

TO SUBSCRIBE, contact TheCanvass@ncsl.org

Exhibit 17

SECOND DECLARATION OF Harry R. Lewis

I, Harry Lewis, declare as follows:

1. My name is Harry R. Lewis.
2. I am Gordon McKay Professor of Computer Science at Harvard University. I have served on the faculty at Harvard for 44 years, a span which includes terms as Dean of the College and as interim Dean of the John A. Paulson School of Engineering and Applied Sciences.
3. I am the author of six books and numerous articles on various aspects of computer science, education, and technology.
4. I am a member of the Electronic Privacy Information Center (EPIC) advisory board.
5. On July 5, 2017, at approximately 6 pm EDT, I undertook to review the security of the website "safe.amrdec.army.mil," recommended by the Vice Chair of the Presidential Advisory Commission on Election Integrity in the letter of June 28, 2017 to state election officials, for the delivery of voter roll data.
6. This is the same website that the Vice Chair described in his July 5, 2017 declaration in this matter as "a secure method of transferring large files up to two gigabytes (GB) in size."

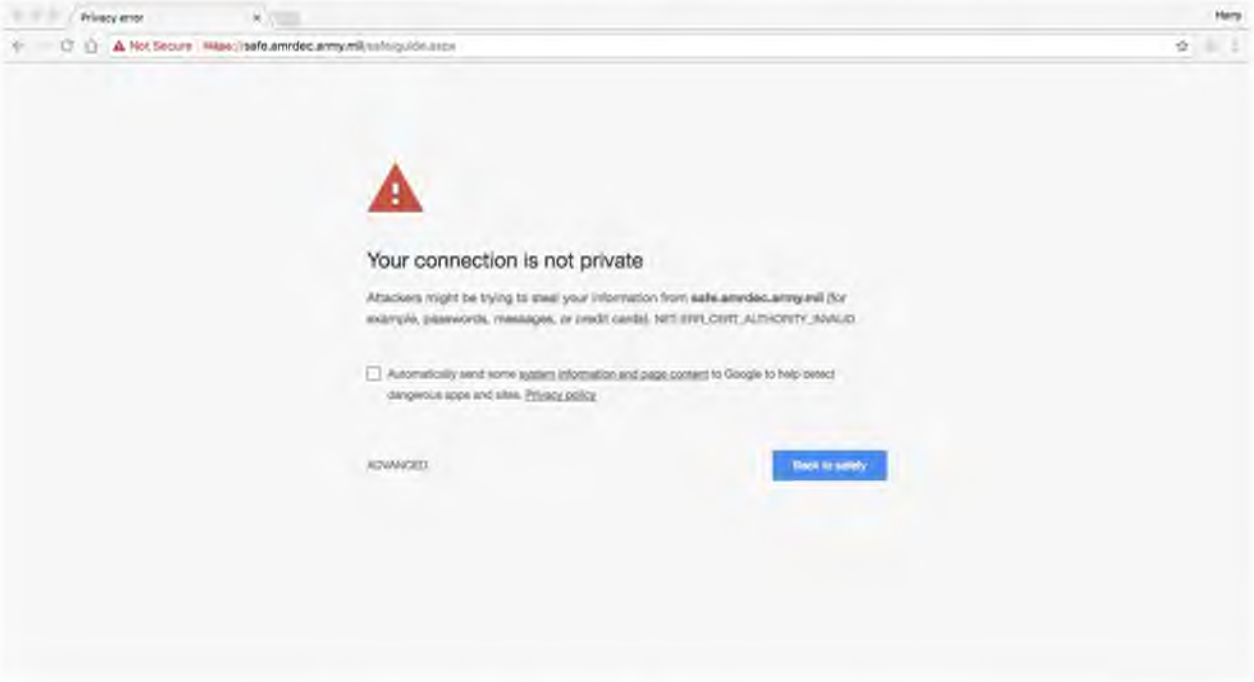
7. The Google Chrome browser returned an error message with a bright red warning mark, which stated, "Your connection is not private – Attackers might be trying to steal your information from **safe.amrdec.army.mil** (for example, passwords, messages, or credit cards)."
8. The Apple Safari browser returned an error message, which stated "Safari can't verify the identity of the website 'safe.amrdec.army.mil.' The certificate for this website is invalid. You might be connecting to a website that is pretending to be 'safe.amrdec.army.mil,' which could put your confidential information at risk."
9. It is my opinion that "safe.amrdec.army.mil" is not a secure website for the transfer of personal data.
10. I have attached to this affidavit contemporaneous screen shots of the responses from the Google Chrome browser and the Apple Safari browser I observed

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed July 5, 2017

Harry R. Lewis

1. Screen shot of Google Chrome browser message



2. Screen shot of Apple Safari browser message

Exhibit 18

U.S. General Services Administration

Privacy Impact Assessments (PIA)

GSA collects, maintains and uses personal information on individuals to carry out the agency's mission and responsibilities and to provide services to the public. By federal law and regulation, privacy issues and protections must be considered for information technology systems that contain any personally identifiable information. GSA uses the Privacy Impact Assessment (PIA) as a key tool in fulfilling these legal and regulatory obligations. By conducting PIAs, GSA ensures that:

- The information collected is used only for the intended purpose;
- The information is timely and accurate;
- The information is protected according to applicable laws and regulations while in GSA's possession;
- The impact of the information systems on individual privacy is fully addressed; and
- The public is aware of the information GSA collects and how the information is used.

PIA Systems

System Title	Acronym/Short Name
ACMIS	ACMIS [PDF - 222 KB]
Challenge.gov	Challenge.gov [DOC - 206 KB]
Childcare Subsidy	CCS [PDF - 329 KB]
Citizen Engagement Platform	CEP [DOC - 100 KB]
ClearPath Hosting Services	GSA FSS-13 [PDF - 189 KB]
Controlled Document Tracker	CDT [PDF - 107 KB]
Customer Engagement Organization	CEO [DOC - 120 KB]
Data.gov	Data.gov [PDF - 300 KB]
Data Leakage Prevention	DLP [PDF - 173 KB]
Digital.gov	Digital.gov [PDF - 474 KB]
eGOV Jobcenter	eGOV Jobcenter [PDF - 199 KB]
eLease	eLease [PDF - 144 KB]
Electronic Acquisition System - Comprizon	EAS-Comprizon [PDF - 158 KB]
Electronic Document Management Software	EDMS [PDF - 49 KB]
EMD	EMD [PDF - 202 KB]
E-PACS	E-PACS [PDF - 48 KB]
E-Travel Carlson Wagonlit Government Travel E2 Solutions	E2Solutions [PDF - 174 KB]
E-Travel Northrop Grumman Mission Solutions - GovTrip	E-Travel GovTrip [PDF - 227 KB]
FAI On-Line University	FAI [PDF - 113 KB]
FAR Data Collection Pilot	FAR [PDF - 51 KB]
FBO	FBO [PDF - 489 KB]
Federal Personal Identity Verification Identity Management System	PIV IDMS [PDF - 222 KB]
ImageNow	ImageNow [PDF - 145 KB]
JP Morgan Chase	JP Morgan [PDF - 55 KB]
Login.gov	Login.gov [PDF - 196 KB]
National Contact Center (NCC)	NCC [PDF - 172 KB]
Office of Inspector General Information System	OIGMIS [PDF - 161 KB]
Office of Inspector General Counsel Files	GSA/ADM-26 [DOC - 38 KB]

18-F-1517//1008

System Title	Acronym/Short Name
OGC Case Tracking	OGC [PDF - 3 KB]
Open Government Citizen Engagement Tool	OGC Engagement [PDF - 384 KB]
ORC	ORC [PDF - 211 KB]
Payroll Accounting and Reporting (PAR)	PAR [PDF - 245 KB]
Pegasys	Pegasys [PDF - 54 KB]
PPFM 8 Chris	PPFM 8 [PDF - 65 KB]
Sales Automation System	SASy [DOC - 104 KB]
Social Media Platforms	Social Media [PDF - 84 KB]
STAR	STAR [DOC - 259 KB]
System for Award Management (SAM)	SAM [DOC - 39 KB]
The Museum System	TMS [PDF - 141 KB]
Transit	Transit [PDF - 195 KB]
USA.gov	USA.gov [PDF - 424 KB]
USAccess	USAccess [PDF - 240 KB]

CONTACTS

GSA Privacy Act Officer

- View Contact Details

PIA POLICY

- 1878.2A CIO P - Conducting Privacy Impact Assessments (PIAs) in GSA

PIA TEMPLATES

- PIA Template
- PIA template for Agency Use of Third-Party Websites and Applications

Exhibit 19

U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

FINAL REPORT:

Audit of U.S. Election Assistance Commission's Compliance with Section 522 of the Consolidated Appropriations Act 2005

Report No.
I-PA-EAC-04-12
May 2013

18-F-1517//1011

U.S. ELECTION ASSISTANCE COMMISSION
Office of Inspector General

May 7, 2013

TO: Alice Miller,
Acting Executive Director and Chief Operating Officer

FROM: Curtis W. Crider
Inspector General

SUBJECT: Review of the U.S. Election Assistance Commission Compliance with Section 522 of the Consolidated Appropriations Act 2005

We contracted with the independent certified public accounting firm of CliftonLarsonAllen, LLP to perform an audit of EAC's compliance with protection of personal data in an identifiable form. The audit included assessing compliance with applicable federal security and privacy laws and regulations as well as assessing the privacy and data protection procedures used by EAC as they relate to the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005. The contract required that the audit be performed in accordance with generally accepted government auditing standards. Attached is a copy of the final report.

In response to the draft report dated February 27, 2013, the EAC generally agreed with the report which included providing expected completion dates for each of the recommendations.

The legislation as amended, creating the Office of Inspector General (5 U.S.C. § App. 3) requires semiannual reporting to Congress on all inspection and evaluation reports issued, actions taken to implement recommendations, and recommendations that have been implemented. Therefore, a summary of this report will be included in our next semiannual report to Congress.

If you have any questions regarding this report, please call me at (202) 566-3125.

Copy to: Mohammed Maeruf, CIO
Annette Lafferty, CFO
Sheila Banks, PO

U.S. ELECTION ASSISTANCE COMMISSION (EAC)

Report on the 2012 Review of EAC's Compliance with Section 522 of the Consolidated Appropriations Act 2005

(Policies, Procedures & Practices of Personally Identifiable Information)

April 25, 2013

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

Mr. Curtis Crider
Office of the Inspector General
U.S. Election Assistance Commission
1225 New York Avenue NW, Suite 1100
Washington, DC 20005

Dear Mr. Crider,

We are pleased to present our report on the U.S. Election Assistance Commission's (EAC) compliance with protection of personal data in an identifiable form. This review included assessing compliance with applicable federal security and privacy laws and regulations as well as assessing the privacy and data protection procedures used by EAC as they relate to the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005. The objective of our review was to determine whether EAC's stated privacy and data protection policies and procedures for personal information of employees and the public are adequate and effective and in compliance with Section 522 of the Appropriations Act of 2005.

We interviewed key personnel involved in the identifying and protecting personally identifiable information and reviewed documentation supporting EAC's efforts to comply with federal privacy and security laws and regulations.

This audit was performed between November 2012 to January 2013 at the EAC office in Washington, District of Columbia. We conducted this performance audit with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We appreciate the opportunity to have served you once more and are grateful for the courtesy and hospitality extended to us by EAC personnel. Please do not hesitate to call me at (301) 931-2050 or email at George.fallon@cliftonlarsonallen.com if you have questions.

Sincerely,

CLIFTONLARSONALLEN LLP

CliftonLarsonAllen LLP

Calverton, Maryland
April 25, 2013

Table of Contents

Executive Summary

Based upon our review, EAC has made improvements to strengthen controls over the security of Personally Identifiable Information (PII) including conducting Privacy Impact Assessments (PIA), appointed a senior agency official for privacy and privacy officer, and developed formalized policies and procedures for PII, however more work remains to be accomplished.

Specifically, EAC was not fully compliant with Section 522 of the Consolidated Appropriations Act 2005 requirements, including:

- Effective encryption mechanisms to appropriately protect agency information, including PII were not implemented;
- Formalized PII usage reports were not submitted to the Office of Inspector General (OIG); and
- EAC Records Management Processes and Procedures Standard Operating Procedures were not formally documented.

Introduction

On December 8, 2004, the President signed into law H.R. 4818, *Consolidated Appropriations Act, 2005* (Public Law 108-447). Title V, Section 522 of this act mandates the designation of a senior privacy official, establishment of privacy and data protection procedures, a written report of the agency's use of information in an identifiable form,[1] an independent third party review of the agency's use of information in an identifiable form, and a report by the Inspector General to the agency head on the independent review and resulting recommendations. Section 522 (d) (3) requires the Inspector General to contract with an independent third party privacy professional to evaluate the agency's use of information in an identifiable form, and the privacy and data protection procedures of the agency. The independent review is to include (a) an evaluation of the agency's use of information in identifiable form, (b) an evaluation of the agency's privacy and data protection procedures, and (c) recommendations on strategies and specific steps to improve privacy and data protection management. Section 522 requires the agency to have an independent third party review at least every 2 years and requires the Inspector General to submit a detailed report on the review to the head of the agency. The third party report and the related Inspector General report are to be made available to the public, i.e. internet availability.

[1] Identifiable form is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Personally identifiable information (PII) has a similar meaning and will be the term used throughout this document.

18-F-1517//1016

Scope and Methodology

Our audit objectives were to evaluate and report on whether the EAC had established adequate privacy and data protection policies and procedures governing the collection, use, disclosure, transfer, storage and security of information relating to agency employees and the public in accordance with Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005.

Our audit scope included the review of EAC documents, and a walkthrough of how PII data is received, processed and stored in electronic and manual form at EAC headquarters in Washington, DC. The following specific procedures were performed to complete the survey assessment:

- Issued a document request list detailing the initial information needed for the audit.
- Reviewed any baseline documentation prepared by EAC to gain a preliminary high level understanding of information in an identifiable form and its use throughout EAC.
- Identified key individuals with responsibility or control over privacy data collected, maintained or processed throughout EAC.
- Evaluated existing work performed by the EAC, the OIG or third parties.
- Reviewed all available documentation related to audits regarding the EAC's implementation and compliance with privacy policy, and practices.
- Coordinated administrative, technical and key logistical aspects of the audit with OIG.
- Obtained permission from the OIG and management to review working papers, documentation, and reports at agreed-upon dates, times and locations; and perform interviews as needed to establish an understanding of missing or incomplete support for the purposes of conducting the privacy audit.
- Obtained an understanding of EAC's privacy and data protection policies and procedures for personal information of EAC employees, contractors and the public.
- Identified and documented risks in EAC's operations for effectively identifying securing and protecting privacy data.
- Analyzed EAC's internal controls related to processes to safeguard privacy data, related policies and procedures, and records management.
- Tested significant controls to determine whether those controls are operating effectively to mitigate any identified risk.
- Issued Notice of Findings and Recommendations (NFRs) to EAC and discussed results with EAC and OIG.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

18-F-1517//1017

Audit Findings and Recommendations

1. ***EAC had not implemented effective encryption mechanisms to appropriately protect agency information, including PII.***

   We noted that EAC had not implemented effective encryption to appropriately protect agency information, including PII. Specifically, the following was noted:

   - EAC did not employ encryption of all data stored on employee desktops or laptops. Additionally, we noted several instances where PII, including names, addresses, phone numbers and social security numbers, were located on the network and not password protected or encrypted.
   - Backup tapes were not encrypted prior to being sent off-site.

   We understand that EAC issued encrypted flash drives to staff, who are required to save sensitive or PII data on these flash drives before removal from the office. Also, EAC employees are required to utilize a designated encryption tool to store the data on their laptops.

   Although all data stored on EAC laptops were not encrypted, we understand that all laptops are protected and monitored by a third party vendor responsible for monitoring the use of each laptop. In the event the laptop is lost or stolen, this vendor is capable of wiping the drive remotely as soon as they identify the computer online. EAC personnel could remotely access their shared drives via VPN and their email by means of a secured web site (SSL) using an Online Web Application.

   EAC's Office of the Chief Information Officer (OCIO), backs up data using a password protected tool that requires using the same password to restore any data. In support of EAC's Disaster Recovery effort, PII data is encrypted by data owners prior to backing up the data to a tape drive and sending it to an offsite location for storage.

   EAC management is presently developing a plan to upgrade workstations and laptops to an operating system platform, which has full-disk encryption capabilities. To address our recommendations, the OCIO and Privacy Officer have indicated they will perform a full scale review of the agency's shared drive to detect unprotected PII and ensure that files and folders are properly protected. At the same time, the SAOP will evaluate the backup device encryption capability of all backup tapes transported offsite for storage.

   Section 1.2 of the *EAC Encryption Key Management* policy states, "all agency data on laptop and portable storage devices (e.g., USB flash drives, external hard drives) must be encrypted with a FIPS 140-2 certified encryption module." Additionally, section 1.3 states "if it is a business requirement to store PII on EAC user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, person digital assistants and Black berries, PII must be encrypted using a FIPS 140-2 certified encryption module."

   National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, security control MP-5, states the following regarding media transport:

18-F-1517//1018

The organization:

a. Protects and controls [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-defined security measures*]; Control Enhancement:

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

EAC employees are encouraged by management to utilize the zipping tool, as an encryption mechanism for storing PII on laptops and other mobile devices; however, files must be stored on the EAC network prior to being compressed and encrypted. EAC is planning to move to the Windows 7 operating system which has built encryption. Additionally, the ability to encrypt backup tapes is available; however, it is a manual feature which EAC can turn on and off. The EAC encryption key was created during the audit period and use was unable to be verified. By not encrypting data, EAC is at an increased risk of data loss or theft.

Recommendations

We recommend EAC management:

1) Develop and implement a plan to implement encryption to all data stored on agency laptops and workstations.
2) Perform a review for unprotected PII stored on the network share drives to ensure files are adequately protected.
3) Implement a validation process to ensure encryption of all backup tapes being transported off-site for storage.

2. Formalized PII usage reports were not submitted to the OIG in accordance with Section 522 of the Consolidated Appropriations Act of 2005.

We noted that EAC management did not provide written PII usage reports to the OIG.

Section 522 of the *Consolidate Appropriations Act of 2005* states, "each agency shall prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report. By signing the report the privacy officer also verifies that the agency is only using information in identifiable form as detailed in the report." (5 U.S.C. § 552a(c))

EAC completes the annual FISMA review which requires the agency to report on information privacy; although the FY 2012 FISMA audit and report did not address the agency's controls surrounding the protection of privacy data. Furthermore, management was unaware of the requirement to complete reports to provide to the OIG of their use and collection of PII, and their adherence of agency policy and regulations.

18-F-1517//1019

Without periodic reviews of agency use of PII, EAC may be unaware of the information that is being collected, used, and stored by the agency; therefore, the agency may inadvertently apply insufficient security controls to adequately protect that information.

Recommendation

We recommend EAC management 1) perform an inventory of EAC's PII data and how it is used within the agency and 2) document and implement a process for the Privacy Officer to periodically report to the Office of Inspector General on the Agency's use of information in an identifiable form, and verify compliance with privacy and data protection policies and procedures.

3. ***The EAC Records Management Processes and Procedures Standard Operating Procedure was not formally documented***

We noted that EAC had not finalized the Records Management Processes and Procedures Standard Operating Procedure as they were in the process of coordinating completion with National Archives and Records Administration (NARA). However, if procedures are not formally documented related to records management, documents may not be adequately encrypted or secured, additionally EAC is at an increased risk of data loss or theft of these records.

We understand that the draft of EAC's Records Management Processes and Procedures Standard Operating Procedures is currently being reviewed by the agency's Acting Executive Director and Chief Operating Officer, Senior Agency Official for Privacy, Privacy Officer, and outside counsel. Once comments have been agreed upon, they will be incorporated into the document and the SOP will be finalized.

Section 522 of Public Law 108-447 states as part of bullet (b)(1), "Within 12 months of enactment of this Act, each agency shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. Such procedures shall be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002.

Recommendation

We recommend EAC finalize and implement the Records Management Processes and Procedures Standard Operating Procedure.

18-F-1517//1020

Conclusions and Recommendations

Based upon our review, EAC has made improvements since the last Privacy audit to strengthen controls over the security of PII including conducting PIA, appointing a senior agency official for privacy and privacy officer, and developing formalized policies and procedures for PII, however more work remains to be accomplished. To become fully compliant with Section 522 of the Consolidated Appropriations Act 2005, EAC needs to ensure privacy role based training is performed, encryption controls to secure PII data stored on desktops, laptops and backup tapes are strengthened, and an ongoing review of and reporting to the OIG of PII usage within the agency and the finalization of records management policies. We recommend EAC management:

- Develop and implement a plan to apply data encryption to all agency laptops and workstations.
- Perform a review for unprotected PII stored on the network share drives to ensure files are adequately protected.
- Implement a validation process to ensure encryption of all backup tapes being transported off-site for storage.
- Perform an inventory of EAC's PII and how it is used within the agency.
- Document and implement a process for the Privacy Officer to periodically report to the Office of Inspector General on the Agency's use of information in an identifiable form, and verify compliance with privacy and data protection policies and procedures.
- Finalize and implement the Records Management Processes and Procedures Standard Operating Procedure.

18-F-1517//1021

Agency Response and OIG Comments

1. **EAC had not implemented effective encryption mechanism to appropriately protect agency information, including PII.**

   Management Response
   Management initially disagreed with this finding related to the recommendation for full disk encryption, however also indicated the current use of encrypted flash drives and planned projects including operating system upgrades, data encryption implementation, review of all shared drives for unsecured PII and a reconfiguration project to mitigate the risks identified.

   OIG Comments
   Revisions were made to the finding and recommendation within this report to address management's concerns related to full disk encryption. Management subsequently concurred with revised wording to data encruption.

2. **Formalized PII usage reports were not submitted to the OIG in accordance with Section 522 of the Consolidated Appropriations Act of 2005.**

   Management Response
   Management agreed with the finding and recommendation and plans to conduct an inventory of EAC's PII and submit a PII usage report to the IG by the first week of July 2013.

   OIG Comments
   Management concurred with our finding and recommendation.

3. **The EAC Records Management Processes and Procedures Standard Operating Procedure (SOP) was not formally documented.**

   Management Response
   Management agreed with the finding and recommendation and indicated EAC's Records Management Standard Operating Processes and Procedures was signed and approved on April 4, 2013.

   OIG Comments
   Management concurred with our finding and recommendation.

18-F-1517//1022

U.S. ELECTION ASSISTANCE COMMISSION
1201 New York Avenue, NW, Suite 300
Washington, DC 20005

Memorandum April 9, 2013

To: Arnie Garza
Assistant Inspector General for Audits

From: Alice Miller
Acting Executive Director & Chief Operating Officer

Subject: 2012 Review of the U.S. Elections Assistance Commission Compliance with Section 522 of the Consolidated Appropriations Act 2005

This memorandum transmits the U.S. Election Assistance Commission's (EAC) responses to the recommendations resulting from the audit performed by CliftonLarsonAllen (CLA) between November 2012 and January 2013. As stated in the draft report, the purpose of the audit was to review EAC's compliance with Section 522 of the Consolidated Appropriations Act 2005.

We are pleased that CLA notes the proactive and significant progress that EAC's Privacy Act Program has made in addressing our statutory responsibilities. We consider privacy to be a matter of great importance and have undertaken significant efforts to ensure compliance.

This memorandum: (1) identifies management's agreement and disagreement with the recommendations; and (2) identifies actions that EAC will take to address the recommendations.

EAC's response to each CLA recommendation follows:

1. ENCRYPTION MECHANISMS

Recommendation: Develop and implement a plan to apply full-disk encryption to agency laptops and workstations. Perform a review for unprotected PII stored on the network share drives to ensure files are adequately protected. Implement a validation process to ensure encryption of all backup tapes being transported off-site for storage.

Management Response: We disagree. To administer internal security controls to protect sensitive and PII data, EAC issued encrypted flash drives to staff. Sensitive and PII data must be encrypted and saved on the hard drives on the server and the flash drives by the information owner.

As indicated in the audit report, efforts are being made by management to safeguard PII data. Current projects include:

- Developing a plan to upgrade workstations and laptops to Windows 7 and utilizing an encryption software application for the partitioned full-disk encryption of EAC workstations and laptops. Sample testing is currently underway.

- Partitioning the disk, thereby, separating the operating system (OS) from the data section. Since the OS does not have to be encrypted, the section containing data will be encrypted on all EAC laptops and workstations.

The Senior Agency Officer of Privacy (SAOP) and the Privacy Officer (PO) will perform a full scale review of the agency's shared drive to ensure that files and folders are properly protected and security access permissions are updated. During this process, active and inactive files will be identified to facilitate the reconfiguration of the shared drive. Active files that can be viewed by all EAC staff will be placed in an Access Central folder; whereas, active files containing PII and sensitive data will be placed in Division folders and accessible via security access permissions. Inactive files will be archived, by division, and will also require security access permissions. To that end, the reconfiguration project will (1) provide increased space on the shared drive, (2) decrease the amount of time it takes to back up the t-drive, and (3) facilitate encryption of all backup tapes being transported off-site for storage.

2. PII USAGE REPORTS

Recommendation: We agree. Perform an inventory of EAC's PII data and how it is used within the agency and document and implement a process for the Privacy Officer to periodically report to the Office of Inspector General on the Agency's use of information in an identifiable form, and verify compliance with privacy and data protection policies and procedures.

Management Response: An inventory of EAC's PII and how it is used in the agency will take place during the current Records Management project, which is expected to be completed by the third quarter in FY 2013. The PO will submit a PII usage report to the IG by the first week in July.

3. RECORDS MANAGEMENT STANDARD OPERATING PROCEDURE (SOP)

Recommendation: Finalize and implement the Records Management Processes and Procedures Standard Operating Procedure.

Management Response: We agree. The final draft of EAC's Records Management Standard Operating Processes & Procedures was signed and approved by executive staff on April 4, 2013 and is currently on EAC's t-drive.

Thank you and the auditors for courtesies and assistance that was extended to our staff during the audit.

If you have any questions regarding our responses, please do not hesitate to contact me at (202) 566-3110.

Copy to: Mohammed Maeruf, CIO
Annette Lafferty, CFO
Sheila Banks, PO

MANAGEMENT RESPONSES TO RECOMMENDATIONS

This table presents management's responses to the recommendations in the draft audit report and the status of the recommendations as of the date of report issuance.

Rec. Number	Corrective Action: Taken or Planned/Status	Measure	Expected Completion Date	Responsible Party(ies)	Resolved:* Yes/ No	Open or Closed**
1	EAC workstations and laptops will be upgraded to Windows 7. IT is currently testing the several encryption software applications to support this task Review, restructure, and update security access to agency's shared drive.	Encryption of data contained on partitioned disk. Full-disk encryption is not necessary.	December 31, 2013	Office of Chief Information Officer Privacy Officer	No	Open
2	PII inventory and usage information will be collected along with information for the Records Management project.	Annual PII Usage Reports submitted to the Office of Inspector General (OIG)	July 5, 2013	Records Management Officer Privacy Officer	Yes	Open
3	Implement the Records Management Standard Operating Processes and Procedures	Finalized Records Management Standard Operating Procedure	April 3, 2013	Acting Executive Director, Inspector General, Chief Financial Officer, Chief Information Officer, Privacy Officer	Yes	Closed

* Resolved – (1) Management concurs with the recommendation, and the planned corrective action is **consistent** with the recommendation.
(2) Management does not concur with the recommendation, but planned alternative action is **acceptable** to the OIG.

** Once the OIG determines that the agreed-upon corrective actions have been completed and are effective, the recommendation can be closed.

18-F-1517//1025

OIG's Mission	The OIG audit mission is to provide timely, high-quality professional products and services that are useful to OIG's clients. OIG seeks to provide value through its work, which is designed to enhance the economy, efficiency, and effectiveness in EAC operations so they work better and cost less in the context of today's declining resources. OIG also seeks to detect and prevent fraud, waste, abuse, and mismanagement in these programs and operations. Products and services include traditional financial and performance audits, contract and grant audits, information systems audits, and evaluations.
Obtaining Copies of OIG Reports	Copies of OIG reports can be requested by e-mail. (eacoig@eac.gov). Mail orders should be sent to: U.S. Election Assistance Commission Office of Inspector General 1201 New York Ave. NW - Suite 300 Washington, DC 20005 To order by phone: Voice: (202) 566-3100 Fax: (202) 566-0957
To Report Fraud, Waste and Abuse Involving the U.S. Election Assistance Commission or Help America Vote Act Funds	By Mail: U.S. Election Assistance Commission Office of Inspector General 1201 New York Ave. NW - Suite 300 Washington, DC 20005 E-mail: eacoig@eac.gov OIG Hotline: 866-552-0004 (toll free) FAX: 202-566-0957

Exhibit 20

The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

2 Martin Luther King Jr., Drive
802 West Tower
Atlanta, Georgia 30334

Chris Harvey
DIRECTOR OF ELECTIONS

July 3, 2017

VIA EMAIL
The Honorable Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity
ElectionIntegrityStaff@ovp.eop.gov

RE: Open Records Request Dated June 28, 2017

Dear Secretary Kobach,

This letter is in response to your request dated June 28, 2017 in which you seek the publicly-available voter roll data for Georgia. Under Georgia law (O.C.G.A. § 21-2-225), information on file regarding Georgia's list of electors is required to be available to the public upon request, except that the day and month of birth, social security number, driver's license number, and the locations at which electors applied to vote are confidential and not subject to disclosure.

Two years ago, our office reformed its process of handling public record requests to be more secure. In order to provide the publicly available information, our security protocol requires certain steps to be followed. Upon receipt, our office will prepare the publicly-available list of electors data file. The data file will undergo a thorough review process to ensure confidential information is not included before it is sent by secure means to the Commission. The data file will be encrypted and password protected.

Also, in order to process and send the requested publicly-available records, our office requires pre-payment of the $250 statewide file fee. Please send check or money order payable to the "Georgia Secretary of State" to my attention at the address in the header of this letter.

Sincerely,

Chris Harvey
Director of Elections
Georgia Secretary of State's Office

Exhibit 31

Report Information from ProQuest

July 12 2017 17:47

18-F-1517//1030

Table of contents

18-F-1517//1031 ProQuest

S INTEL HEARING ON RUSSIAN INTERFERENCE IN 2016 ELECTION, PANEL 1

Publication info: Political Transcript Wire ; Lanham [Lanham]21 June 2017.

ProQuest document link

Links: Check SFX for Availability

Full text: (CORRECTED COPY - CORRECTIIONS THROUGHOUT TEXT)

S Intel Hearing on Russian Interference in 2016 Election, Panel 1

JUNE 21, 2017

SPEAKERS: SEN. RICHARD M. BURR, R-N.C. CHAIRMAN SEN. JIM RISCH, R-IDAHO SEN. MARCO RUBIO, R-FLA. SEN. SUSAN COLLINS, R-MAINE SEN. ROY BLUNT, R-MO. SEN. TOM COTTON, R-ARK. SEN. JAMES LANKFORD, R-OKLA. SEN. JOHN CORNYN, R-TEXAS SEN. MARK WARNER, D-VA. VICE CHAIRMAN SEN. RON WYDEN, D-ORE. SEN. MARTIN HEINRICH, D-N.M. SEN. JOE MANCHIN III, D-W.VA. SEN. KAMALA HARRIS, D-CALIF. SEN. DIANNE FEINSTEIN, D-CALIF.

SEN. ANGUS KING, I-MAINE

SEN. JACK REED, D-R.I.

WITNESSES: SAM LILES, ACTING DIRECTOR, OFFICE OF INTELLIGENCE AND ANALYSIS CYBER DIVISION DEPARTMENT OF HOMELAND SECURITY

JEANETTE MANFRA, UNDERSECRETARY OF HOMELAND SECURITY, AND ACTING DIRECTOR, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

BILL PRIESTAP, ASSISTANT DIRECTOR, FBI COUNTERINTELLIGENCE DIVISION

[*] BURR: Today the committee -- committee convenes it's sixth open hearing of 2017, to further examine Russia's interference in the 2016 elections. This is yet another opportunity for the committee and the American people to drill down on this vitally important topic.

In 2016 a hostile foreign power reached down to the state and local levels to touch voter data. It employed relatively sophisticated cyber tools and capabilities and helped Moscow to potentially build detailed knowledge of how our elections work. It was also another example of Russian efforts to interfere into a democracy with the goal of undermining our system.

In 2016, we were woefully unprepared to defend and respond and I'm hopeful that we will not be caught flatfooted again.

Our witnesses are here to tell us more about what happened in 2016, what that tells us about Russian intentions, and what we should expect in 2018 and 2020. I'm deeply concerned that if we do not work in lockstep with the states to secure our elections, we could be here in two or four years talking about a much worse crisis.

The hearing will feature two panels.

First panel will include expert witnesses from DHS and FBI to discuss Russian intervention in 2016 elections and U.S. government efforts to mitigate the threat.

The second panel will include witnesses from the Illinois State Board of Elections, the National Association of State Elections and Directors, National Associations of Secretary of States and an expert on election security to give us their on-the-ground perspective on how federal resources might be brought to bear on this very important issue.

For our first panel, I'd like to welcome our witnesses today: Dr. Samuel Liles, acting director of Cyber Division within the Office of Intelligence and Analysis at the Department of Homeland Security; Jennifer (sic) Manfra, acting deputy undersecretary, National Protection and Programs Dictorate (sic), also at DHS.

And Jeanette, I think I told you next time you came I did not want "acting" in front of your name. So now I've

18-F-1517//1032

publicly said that to everybody at DHS. Hopefully next time that will be removed.
And Bill Priestap. Bill's the assistant director for Counterintelligence Division at the Federal Bureau of Investigation.
Bill, I want to thank you for the help that you have personally provided to the investigative staff of this committee, as we've worked through, so far, over five and a half months of our investigation into the 2016 elections.
As you're well aware, this committee is in the midst of a comprehensive investigation on the specific issue: the extent to which Russian government under the direction of President Putin conducted intelligence activities, also known as Russian active measures, targeted at the 2016 U.S. elections. The intelligence community assesses that, while Russian influence obtained and maintained access to elements of multiple U.S. state and local election boards, those systems were not involved in vote tallying.
During the first panel, I would like to address the depth and the breadth of Russian government cyber activities during the 2016 election cycle, the efforts of the U.S. government to defend against these intrusions, and the steps that DHS and FBI are taking to preserve the foundation of our democracy's free and fair elections in 2018 and beyond.
I thank all three of our first witnesses.
I turn to the vice-chairman.
WARNER: Thank you, Mr. Chairman.
And welcome to the witnesses.
And, Bill, thank you again for all the work you've done with us.
WARNER: We all know that in January, the entire intelligence community reached the unanimous conclusion that Russia took extraordinary steps to intervene in our 2016 presidential elections. Russia's interference in our elections in 2016 I believe was a watershed moment in our political history.
This was one of the most significant events I think any of us on this dais will be asked to address in our time as senators. And only with a robust and comprehensive response will we be able to protect our democratic processes from even more dramatic incursions in the future.
Much of what the Russians did at this point, I think at least in this room, is -- was well known: spreading fake news, flooding social media, hacking personal e-mails and leaking them for maximum political benefit.
Without firing a shot and at minimal cost, Russia sowed chaos in our political system and undermined faith in our democratic process. And as we've heard from earlier witnesses, sometimes that was aided by certain candidates, in terms of their comments about the legitimacy of our democratic processes.
Less well understood, though, is the intelligence community's conclusion that they also secured and maintained access to elements of multiple U.S. state and local electoral boards.
Now, again, as the chairman has said, there's no reason to doubt the validity of the vote totals in the 2016 election. However, DHS and the FBI have confirmed -- and I'm going to come back to this repeatedly -- only two intrusions into the voter registration databases, in both Arizona and Illinois, even though no data was modified or deleted in those two states.
At the same time, we've seen published reports that literally dozens -- I've seen one published report that actually said 39 states -- were potentially attacked.
Certainly is good news that the attempts in 2016 did not change the results of that election. But the bad news is this will not be their last attempt. And I'm deeply concerned about the danger posed by future interference in our elections and attempts by Russian to undermine confidence in our whole electoral system.
We saw Russian -- we saw recently -- and this was just not happening here, obviously -- we saw recently Russian attempts to interfere in the elections in France. And I thank the chairman that next week we'll be having a hearing on some of these Russian efforts in Europe.
We can be sure that Russian hackers and trolls will continue to refine their tactics in the future -- future,

especially if there's no penalty for these malicious attacks.

That's again, one reason I think that the Senate voted so overwhelmingly last week, and I thank all my colleagues for that 97-2 vote to strengthen our sanctions on Russia. I hope that that action sends a strong message to Mr. Putin that there will be a heavy price to pay for attacks against the fundamental core of our democratic system.

Make no mistake, it's likely that we'll see more of these attacks not just in America but against our partners. I heard this morning coming on the radio that the Russians are already actively engaged in the German election cycle, which takes place this fall.

Now, some might say, "Well, why -- why the urgency?"

I can assure you, you know, we have elections in 2018, but in my home state of Virginia, we have statewide elections this year. So this needs a sense of urgency.

The American electoral election process, the machinery, the Election Day manpower, the actual counting and reporting primarily is a local and state responsibility. And in many states, including my own, we have a very decentralized approach, which can be both a strength and a weakness.

WARNER: In Virginia, for instance, decentralization helps deter large-scale hacking or manipulation, because our system is so diffuse. But Virginia localities use more than a dozen different types of voting machines, none of which are connected to the internet while in use, but we have a number of machine-read -- machine -- reader (ph) machines, so that they -- the tabulations actually could be broken into on an individual machine basis.

All this makes large cyber-attacks on electoral system, because of the diffusion, more difficult. But it also makes maintaining consistent, coordinated cyber defenses more challenging as well.

Furthermore, states may be vulnerable when it comes to the defense of voter registration and voter history databases. That's why I strongly believe that that the threat requires us to harden our cyber defenses and to thoroughly educate the American public about the danger.

Yesterday, I wrote to the secretary of homeland security. I urged DHS to work closely with state and local election officials to disclose publicly -- and I emphasize publicly -- which states were targeted. Not to embarrass any states, but how can we put the American public on notice when we've only revealed two states, yet we have public reports that there are literally dozens? That makes absolutely no sense.

I know it is the position of DHS that since the states were victims, it is their responsibility. But I cannot believe that this was an attack on physical infrastructure in a variety of states, there wouldn't be a more coordinated response.

We are not making our country safer if we don't make sure that all Americans realize the breadth and the extent of what the Russians did in 2016, and, frankly, if we don't get our act together, what they will do in an -- a even more dramatic form in 2018 and 2020.

And candidly, the idea of this kind of bureaucratic, "Well, it's not my responsibility, not my job," I don't believe is an acceptable decision.

So, I'm going to hope from our witnesses, particularly our DHS -- DHS witnesses, that we hear a plan on how we can get more information into the bloodstream, how we can make sure that we have better best practices, so that all states are doing what's needed.

I'm not urging or suggesting that in any way the federal government intervenes in what is a local and state responsibility. But to not put all Americans on notice, not -- and to have the number of states that were hacked into or attempt to be hacked into still kept secret is -- is just crazy in my mind.

So, my hope is that we will get some answers. I -- I do want to thank the fact that in January, DHS did designate the nation's electoral infrastructure as critical infrastructure. That's important. But if we call it critical infrastructure but then don't tell the public how many states were attacked or potentially how many could be attacked in the next cycle, I don't think we get to where we need to be.

So, we're going to have -- see more of this. This is the new normal. I appreciate the chairman for holding this

hearing. And I'm going to look forward very much to getting my questions answered.
Thank you.
BURR: Thank you, Vice Chairman.
With that, Dr. Liles, I understand you're going to go first. The floor is yours.
LILES: Chairman Burr, Ranking Member Warner and distinguished members of the committee, thank you for the invitation to be here.
My name is Sam Liles. I represent the Cyber Analysis Division of the Department of Homeland Security's Office of Intelligence and Analysis. Our mission is to produce cyber-focussed intelligence, information and analysis, represent our operational partners like the NCCIC to the intelligence community, coordinate and collaborate on I.C. products, and share intelligence and information with our customers at the lowest classification possible.
We are a team of dedicated analysts who take threats to the critical infrastructure of the United States seriously.
I'd like to begin by clarifying and characterizing the threat we observed to the election infrastructure in the 2016 election.
LILES: Prior to the election, we had no indication that adversaries or criminals were planning cyber operations against the U.S. election infrastructure that would change the outcome of the coming U.S. election.
However, throughout spring and early summer 2016, we and other -- others in the I.C. began to find indications that the Russian government was responsible for widely reported compromises and leaks of e-mails from U.S. political figures and institutions.
As awareness of these activities grew, DHS began in 2016 to receive reports of cyber-enabled scanning and probing of election- related infrastructure in some states.
From that point on, I&A began working to gather, analyze and share additional information about the threat. I&A participated in red team events, looking at all possible scenarios, collaborated and co-authored production with other intelligence community members and the National Intelligence Council. We provided direct support to the department's operational cyber center, the National Cyber Security and Communications Integration Center and worked hand-in-hand with the state and local partners to share threat information related to their networks.
By late September, we determined that internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors.
It is important to note that none of these systems were in involved in vote tallying. Our understanding of that targeting, augmented by further classified reporting is that's still consistent with the scale and scope.
This activity is best characterized as hackers attempting to use commonly available cyber tools to exploit known system vulnerabilities. This vast majority of the -- the activity we observed was indicative of simple scanning for vulnerabilities, analogous to somebody walking down the street and looking to see if you are home.
A small number of systems were unsuccessfully exploited, as though somebody had rattled the doorknob but was unable to get in, so to speak.
Finally a small number of the networks were successfully exploited. They made it through the door. Based on activity we observed, DHS made a series of assessments. We started out with, we had no indication prior to the election that adversaries were planning cyber operations against election infrastructure that would change the outcome of the 2016 election. We also assessed that multiple checks and redundancies in U.S. election infrastructures, including diversity of systems, non-internet- connected voting machines, pre-election testing and processes for media, campaign and election officials to check, audit and validate the results -- all these made it likely that cyber manipulation of the U.S. election systems intended to change the outcome of the national election would be detected.
We also finally assessed that the types of systems Russian actors targeted or compromised were not involved in vote tallying.
While we continue to evaluate any and all new available information, DHS has not altered any of these prior assessments. Having characterized the threat as we observed it, I'll stop there to allow my NPPD colleague

Jeanette Manfra to talk about more about DHS is working with election systems to add security and resiliency. I look forward to answering your questions.

BURR: Thank you.

Ms. Manfra?

MANFRA: Thank you, sir.

Chairman Burr, Vice Chairman Warner, members of this committee, thank you for today's opportunity to represent the men and women that serve in the Department of Homeland Security.

Today I'm here to discuss the department's mission to reduce and eliminate threats to the nation's critical physical and cyber infrastructure, specifically as it relates to our election.

Our nation's cyber infrastructure is under constant attack. In 2016, we saw cyber operations directed against U.S. election infrastructure and political entities. As awareness of these activities grew, DHS and its partners provided actionable information and capabilities to help -- help election officials identify and mitigate vulnerabilities on their networks.

MANFRA: Actionable information led to detection of potentially malicious activity affecting internet-connected election-related networks, potentially targeted by Russian cyber actors in multiple states. When we became aware of detected activity, we worked with the affected entity to understand if a successful intrusion had in fact occurred.

Many of these detections represented potentially malicious vulnerability scanning activity, not successful intrusion. This activity, in partnership with these potential victims and targets, enhanced our situational awareness of the threat and further informed our engagement with state and local election officials across the country.

Given the vital role that elections have in a free and democratic society, on January 26 of this year, the former secretary of homeland security established election infrastructure as a critical infrastructure sub-sector. As such, DHS is leading federal efforts to partner with state and local election officials, as well as private sector vendors, to formalize the prioritization of voluntary security- related assistance, and to ensure that we have the communications channels and protocols, as Senator Warner discussed, to ensure that election officials receive information in a timely manner and that we understand how to jointly respond to incidents.

Election infrastructure now receives cybersecurity and infrastructure protection assistance similar to what is provided to other critical infrastructure, such as financial institutions and electric utilities. Our election system is run by state and local governments in thousands of jurisdictions across the country. Importantly, state and local officials have already been working individually and collectively to reduce risks and ensure the integrity of their elections. As threat actors become increasingly sophisticated, DHS stands in partnership to support their efforts.

Safeguarding and securing cyberspace is a core mission at DHS. Through out National Cybersecurity and Communications Center, or NCCC, DHS assists state and local customers such as election officials as part of our daily operations. Such assistance is completely voluntary. It does not entail regulation or federal oversight. Our role is limited to support.

In this role, we offer three types of assistance: assessments, information and incident response. For the most part, DHS has offered two kinds of assistance to state and local officials: first, the cyber hygiene service for internet facing systems provides a recurring report identifying vulnerabilities and mitigation recommendations; second, our cybersecurity experts can go on-site to conduct risk and vulnerability assessments and provide recommendations to the owners of those systems for how best to reduce the risk to their networks.

DHS continues to share actionable information on cyber threats and incidents through multiple means. For example, we publish best practices for securing voter registration databases and addressing potential threats to election systems. We share cyber-threat indicators, another analysis that network defenders can use to secure their systems.

We partner with the multistate Information Sharing and Analysis Center to provide threat and vulnerability

information to state and local officials. This organization is partially grant-funded by DHS and has representatives that sit on our NCCC floor and can interact with our analysts and operators on a 24/7 basis. They can also receive information through our field-based personnel stationed throughout the country and in partnership with the FBI.

Finally, we provide incident response assistance at request to help state and local officials identify and remediate any possible cyber incident. In the case of an attempted compromise affecting election infrastructure, we will share that technical information with other states to assist their ability to defend their own systems from similar malicious activity.

Moving forward, we must recognize that the nature of risk facing our election infrastructure will continue to evolve. With the establishment of an election infrastructure sub-sector, DHS is working with stakeholders to establish these appropriate coordinating councils and our mechanisms to engage with them. These will formalize our mechanisms for collaboration and ensures long-term sustainability of this partnership. We will lead the federal effort to support election officials with security and resilience efforts.

MANFRA: Before closing, I want to reiterate that we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient. It is diverse, subject to local control and has many checks and balances built in. As the risk environment evolves, the department will continue to support state and local partners by providing information and offering assistance.

Thank you very much for the opportunity to testify, and I look forward to any questions.

BURR: Thank you very much.

Mr. Priestap?

PRIESTAP: Good morning.

Chairman Burr, Vice Chairman Warner, and members of the committee, thank you for the opportunity to appear before you today.

My statement for the record has been submitted. And so rather than restating it, I'd like to step back, and provide you a description of the broader threat as I see it. My understanding begins by asking one question. What does Russia want?

As you well know, during the Cold War, the Soviet Union was one of the world's two great powers. However, in the early 1990's, it collapsed and lost power, stature and much territory. In a 2005 speech, Vladimir Putin, referred to this as a major catastrophe. The Soviet Union's collapse left the U.S. as the sole super power. Since then, Russia has substantially rebuilt, but it hasn't been able to fully regain its former status or its former territory. The U.S. is too strong and has too many alliances for Russia to want a military conflict with us. Therefore, hoping to regain its prior stature, Russia has decided to try to weaken us and our allies.

One of the ways Russia has sought to do this is by influence, rather than brute force. Some people refer to Russia's activity, in this regard, as information warfare, because it is information that Russia uses as a weapon. In regards to our most recent presidential election, Russia used information to try to undermine the legitimacy of our election process. Russia sought to do this in a simple manner. They collected information via computer intrusions and via their intelligence officers, and they selectively disseminated e-mails they hoped would disparage certain political figures and shed unflattering light on political processes.

They also pushed fake news and propaganda. And they used online amplifiers to spread the information to as many people as possible. One of their primary goals was to sow discord and undermine a key democratic principle, free and fair elections.

In summary, I greatly appreciate the opportunity to be here today to discuss Russia's election influence efforts. But I hope the American people will keep in mind that Russia's overall aim is to restore its relative power and prestige by eroding democratic values. In other words, its election-related activity wasn't a one-time event. Russia will continue to pose an influence threat.

I look forward to your questions. Thank you.

BURR: Thank you very much to all of our witnesses. For members, we will proceed by seniority for recognition for up to five minutes. And the chairman will tell you when you have used all your time if you proceed that far. Chair would recognize himself for five minutes.

Yes or no to all three of you. Most important question.

BURR: Do you have any evidence that the votes themselves were changed in any way in the 2016 presidential election?

Dr. Liles?

LILES: No, sir. There was no detected change in the vote.

BURR: Ms. Manfra?

MANFRA: No, sir.

BURR: Mr. Priestap?

PRIESTAP: No, sir.

BURR: Bill, to you. This adversary is determined. They're aggressive and they're getting more sophisticated by the day. The diversity of our election system is a strength, but the intrusions in the state systems also show that Moscow is willing to put considerable resources towards an unclear result.

In 2016, we saw voter data stolen. How could Moscow potentially use that data?

PRIESTAP: They could use the data in a variety of ways. Unfortunately in this setting, I can't go into all of them. I think -- first of all, I think they took the data to understand what it consisted of; what's there, so that they can effect better understand and plan accordingly.

And when I say "plan accordingly," plan accordingly in regards to possibly impacting future elections and/or targeting of particular individuals, but also by knowing what's there and studying it. They can determine is it something they can manipulate or not, possibly, going forward. And there's a couple of other things that wouldn't be appropriate in this setting as well.

BURR: To any of you, you've heard the vice chairman talk about the frustration of publicly talking about how many states. Can you tell the American people why you can't disclose which states and the numbers?

I'll turn to Ms. Manfra first.

MANFRA: Thank you for the question, sir. There are -- through the long history that the department has in working with the private sector and state and local on critical infrastructure and cybersecurity issues, we believe it is important to protect the confidentiality that we have and the trust that we have with that community. So when the entity is a victim of a cyber incident, we believe very strongly in protecting the information around that victim.

That being said, what we can do is take the technical information that we learn from the engagement with that victim and anonymize it so it is not identified as to what that entity or individual is. We can take all the technical information and turn that around and share that broadly with -- whether it's the affected sector or broadly across, you know, the entire country. And we have multiple mechanisms for sharing that.

We believe that this has been a very important key to our success in developing trusted relationships across all of these 16 critical infrastructure sectors.

BURR: Are we prepared today to say publicly how many states were targeted?

MANFRA: We, as of right now, we have evidence of 21 states -- election-related systems in 21 states that were targeted.

BURR: But in no case were actual vote tallies altered in any way, shape or form?

MANFRA: That is correct.

BURR: How did the -- how did the French respond to the Russian involvement in the French elections a month ago? Is that something we followed?

Bill?

PRIESTAP: Senator, from the bureau's standpoint, it's something we followed from afar. We did have

engagement with French officials, but I'm just not at liberty to go into what those consisted of.
BURR: OK, we've -- we've talked about last year. Russia's intent, their target. Let's talk about next year. Let's talk about the '17 elections in Virginia. Let's talk about the '18 elections, congressional, and -- and -- and gubernatorial elections. What are we doing to prepare ourselves with this November and next November?
Ms. Manfra?
MANFRA: Yes, sir.
As we noted, we are taking this threat very seriously. And part of that is identifying this community's critical infrastructure subsector. That's allowed us to prioritize and formalize the engagement with them.
Similar to the 2016 elections, we are identifying additional resources, prioritizing our engagement with them through information sharing products, identifying in partnership, again, with the state and local community, those communication protocols -- how do we ensure that we can declassify information quickly should we need to, and -- and get it to the individuals that need it.
We're also -- have committed to working with state and local officials on incident response playbooks. So, how do they understand where to engage with us, where do we engage with them, and how do we -- are we able to bring the entire resources of the federal government to bear in helping the state and local officials secure their election systems?
BURR: Great.
Vice Chairman?
WARNER: Thank you for the answer. At 21 -- 21 states is almost half the country. We've seen reports that were even higher. I concur with the chairman that the vote totals were not changed. But can you explain to me how we're made safer by keeping the identity of 19 of those states secret from the public? Since Arizona and Illinois have acknowledged they were -- they were attacked?
LILES: Well, sir, I'd bring it back to the earlier points you made about the future elections. One of the key pieces for us within I&A is our ability to work with our partners because of how our collection mechanisms work, it's built on a high level of trust...
(CROSSTALK) WARNER: And if this was -- if this was water systems or power systems, would it be -- would the public be safer by not knowing that their water system or power system in their respective state was attacked?
MANFRA: Sir, I can -- in -- for other sectors, we apply the same principles. When we do have a victim of an incident in the electric sector, or the water sector, we do keep the name of that entity confidential. Some of these sectors do have breach reporting requirements that -- that requires the victims...
(CROSSTALK)
WARNER: Are -- are all 21 of the states that were attacked, are they aware they were attacked?
MANFRA: All of the system owners within those states are aware of the targeting. Yes, sir.
WARNER: At the state level, you could have local registrars and other local officials that -- that there may have been an attempt to penetrate at the state level. And you may have local registrars in the respective state that would not even know that their state had been the subject of Russian activities?
MANFRA: We are currently working with state election officials to ensure communication between the local and the -- and the state...
(CROSSTALK)
WARNER: But at this moment in time, there may be a number of state, local -- state, local election officials that don't know their state were targeted in 2016. Is that right?
MANFRA: The -- the owners of the systems that were targeted do know that they were targeted...
(CROSSTALK)
WARNER: The owners may know, but because we have a decentralized system, many local elective -- I just -- I...

MANFRA: I -- I cannot...
WARNER: ...fundamentally disagree. I understand the notion of victimization.
MANFRA: Yes, sir.
WARNER: But I do not believe our country is made safer by holding this information back from the American public. I got -- I have no interest in trying to embarrass any state.
WARNER: But, you know, if -- if this -- because we -- we've seen this for too long in cyber. We've seen it in the financial industry, and others, where people simply try to sweep this under the rug, and assume they'll go along their way. When we're talking about -- I go back to Liles' initial comments.
We had no idea -- we had no ability to predict this before hand. We had 21 states that were tapped. We've got two that have come forward. While no election results were changed, we do know there were a number of states, perhaps you'll answer this. How many states did the Russians actually exfiltrate data, such as voter registration lists?
MANFRA: Prefer not to go into those details in this forum, sir. I can tell you that we're tracking 21 states that were targeted...
(CROSSTALK)
WARNER: Do the states that had their data exfiltrated by the Russians -- are they aware of that?
MANFRA: Yes, sir.
WARNER: And is there any coordinated response on how we're going to prevent this going forward?
MANFRA: Yes, sir.
WARNER: How do we make sure, if states are not willing to acknowledge that they had vulnerabilities that they were subject to attack -- again, we're in a brave new world here and I understand your position. I'm not trying to -- I'm very frustrated, but I'm not -- I -- I -- I get this notion.
But I think we need a re-examination of this policy. You know, the designation by former Secretary Johnson as critical infrastructure. What does that change in terms of how our operations are going forward? By that designation in January, I appreciated it, but what does that really mean in practical terms, in terms of assistance or information sharing?
MANFRA: What it means for -- it means three things, sir. The first is a statement that we do recognize that these systems are critical to the functioning of American life, and so that is an important statement. The second is, that it formalizes and the -- and sustains, the department's prioritization of engagement with this community. And the last is, it provides a particular protection for sharing of information, in particular, with vendors within the election community. That allows us to have conversations to discuss vulnerabilities with potential systems, that we would not have to disclose.
WARNER: I -- I talked to Secretary Kelly last week, and I hope you'll take this -- at least this Senator's message, back to him. I would like us to get more information. What I've heard today is that, there were 21 states, I appreciate that information, but within those 21 states I have no guarantee that local election officials are aware that their state system may have been attacked, number one.
Number two, we don't know how many states actually had exfiltration. And the final question is, have you seen any stoppage of the Russian activities after the election? Or are they continuing to ping and try to feel out our various election systems?
MANFRA: On the first two questions, sir, I will be happy to get back to you. I spoke to the Secretary this morning and look forward to responding to your letter. On the third question, I'll defer to the FBI.
PRIESTAP: Vice Chairman, I just can't comment on our pending investigations related to the cyber...
(CROSSTALK)
WARNER: You can't say whether the -- so, should the public take away a sense of confidence that the Russians have completely stopped, as of November of 2016, trying to interfere or tap into our electoral systems. Is that what you're saying?

PRIESTAP: That's not what I'm saying, sir. I believe the Russians will absolutely continue to try to conduct influence operations in the U.S., which will include cyber intrusions.
WARNER: Thank you, Mr. Chairman.
BURR: Thank you, Vice Chairman.
To DHS and to the Bureau, a quick question, and if you can't answer it, please go back and get us an answer. Would your agency be opposed to the chair and vice chair sending a letter to the 19 states that have not been publicly disclosed, a classified letter, asking them if they would consider publicly disclosing that they were a target of the last election?
PRIESTAP: Sir, I'd be happy to take that question back to my organization, but I would just add that the role your committee is playing in regards to highlighting the Russian' aims and activities, I think, is critically important for this country.
The Bureau is just trying to balance what -- we'll call it the messaging end of that with doing things that hopefully don't impact what we can learn through our investigations. I know it's a fine -- it's a fine balance but -- but the bottom line is you play a key role in raising awareness of that, and I thank you.
BURR: Fair -- fair -- fair concern, and if both of you would just go back and get back with us, we'll proceed from there.
Senator Risch?
RISCH: Thank you much.
So that the American people can have solid confidence in what you've done, and thank you for what you've done, could you give -- could you give the American people an idea -- if you feel the numbers are classified and that sort of thing, you don't have to go into it.
But the number of people that were involved on DHS and the FBI in this investigation -- can you give us a general idea about that? Whichever one of you want to take that question.
Ms. Manfra?
MANFRA: From a DHS perspective, we did amass quite a few resources both from our intelligence and analysis and our operations analysis. To put a number on it is -- is somewhat challenging but, you know...
(CROSSTALK)
RISCH: Would you say it was substantial?
MANFRA: It was a substantial level of effort.
RISCH: You -- you're confident that you got where you wanted to go when you set out to -- to make this investigation?
MANFRA: Yes, sir. One of our key priorities was developing relationships with that community and getting information out, whether it was to specific victims or broader indicators, that we could share.
We accomplished that. We held multiple sessions. We sent over 800 indicators to the community and so we do believe that -- that we accomplished that. We don't want to let that down at all. We want to continue that level of effort and we intend to continue.
RISCH: And I'm focusing on not what you did after you got the information, but how you got the information. You're confident you got what you needed to appropriately advise everyone in this -- what was going on?
MANFRA: Yes, sir. Yes, we did.
RISCH: Mr. Priestap?
PRIESTAP: This -- the FBI considered this a very grave threat and so we dedicated substantial resources to this effort as well. RISCH: OK. Thank you. To both of you, both agencies again, everyone in this committee knows the specificity and identity of the Russian agencies involved. Are you comfortable in identifying them here today, or do you feel -- still feel that's classified?
PRIESTAP: Yeah. Other what was mentioned in the unclassified version of the intelligence community assessment, I'd rather not go into any of those details.

RISCH: And -- and -- were there any of those agencies identified, any of the Russian intelligence agencies, identified in that?
PRIESTAP: It's my understanding that GIU was identified.
RISCH: Homeland Security, same answer?
LILES: Yes, sir.
RISCH: OK. Thank you much. Let me -- let me ask this question and I come at this from a little different perspective, and I think the American people have the right to know this. From all the work that either of your agencies did, all the people involved, all the digging you did through what -- what the Russians had done and their attempts.
RISCH: Did you find any evidence, direct or circumstantial, to any degree, down to a scintilla of evidence, that any U.S. person colluded with, assisted or communicated with the Russians in their efforts?
Mr. Priestap?
PRIESTAP: And sir, I -- I just can't comment on that today. That falls under the special counsel's purview. And I have to defer to him.
RISCH: Are you aware of any such evidence?
PRIESTAP: And I'm sorry, sir, I just can't comment on that.
RISCH: Ms. -- Ms. Manfra?
MANFRA: Sorry, sir. I cannot also comment on that.
RISCH: Thank you.
Thank you, Mr. Chairman.
BURR: Senator Feinstein?
FEINSTEIN: Thanks very much, Mr. Chairman.
Candidly, I'm very disappointed by the testimony. I mean, we have learned a great deal. And the public has learned a great deal. And it seems to me we have to deal with what we've learned.
Mr. Priestap, is that correct? You have said, and I think quite pointedly, that Russia has decided to weaken us through covert influence rather than brute force. And I think that's a correct assessment, and I think you for having the courage to make it.
Here's a question. To the best of the FBI's knowledge, have they conducted covert influence in prior election campaigns in the United States? If so, when, what and how?
PRIESTAP: Yes, absolutely, they've conducted influence operations in the past. What -- what made this one different, in may regards, was of course, the degree, and then with what you can do through electronic systems today.
When they did it in the past, it was doing things like trying to put in biased or -- or half-true stories, get -- getting stories like that into the press or pamphlets that people were -- will -- would read, so on and so forth. The -- the internet is just -- has allowed Russia to do so much more today than they've even been able to do in the past.
FEINSTEIN: So, you're saying prior campaigns were essentially developed to influence one campaign above another, to denigrate a candidate if she was elected and to support another candidate subtly?
PRIESTAP: Yeah, I -- I'm saying that Russia, for years, has conducted influence operations targeting our elections, yes.
FEINSTEIN: Equal to this one?
PRIESTAP: Not equal to this one. No, ma'am.
FEINSTEIN: OK, here we go. What made this one different?
PRIESTAP: Again, I -- I think the -- the scale -- the scale and the aggressiveness of the effort, in my opinion, made this one different. And again, it's -- it's because of the electronic infrastructure, the internet, what have you, today that -- it allowed Russia to do things that in the past they weren't able to do.
FEINSTEIN: Would you say that this effort was tailored to achieve certain goals?

PRIESTAP: Absolutely.
FEINSTEIN: And what would those goals have been?
PRIESTAP: I think the primary goal in my mind was to sow discord and to try to delegitimize our free and fair election process. I also think another of their goals, which the entire United States intelligence community stands behind, was to denigrate Secretary Clinton and to try to help then -- current President, Trump.
FEINSTEIN: Have they done this on -- in prior elections in which they've been involved?
PRIESTAP: Have they...
(CROSSTALK)
FEINSTEIN: Denigrated a specific candidate and or tried to help another candidate?
PRIESTAP: Yes, ma'am, they have.
FEINSTEIN: And which elections were those?
PRIESTAP: Oh -- I'm sorry, I know there -- I -- I'm sorry, I can't think of an example off the top of my head, but even though -- all the way through the Cold War, up to our most recent election -- in my opinion, they have tried to influence all of our elections since then, and this is a common practice.
FEINSTEIN: Have they ever targeted what is admitted here today to be 21 states?
PRIESTAP: If they have, I am not aware of that. That's a -- that scale is different than what I'm aware of what they tried to do in the past. So again, the scale and aggressiveness here, separates this from their previous activity.
FEINSTEIN: Has the FBI looked at how those states were targeted?
PRIESTAP: Absolutely, ma'am.
FEINSTEIN: And what is your finding?
PRIESTAP: We have a number of investigations open in regards to that. In this setting -- I guess, because they're all still pending investigations, I'd rather not go into those details. The other thing I'd ask you to keep in mind is that we continue to learn things. So, there was some activity we were looking at prior to the election. It's not like when the election was finished our investigation stopped. So as we learn more, we share more.
FEINSTEIN: Do you know if it's the intent of the FBI to make this information public at some point?
PRIESTAP: I -- I think this gets back to an -- an issue the vice-chairman raised, and I -- I guess I want to be clear on my position on it. I think it is critically important to raise awareness about Russia's aims to undermine our democracy, and then their tradecraft and how they do it.
My organization -- part of understanding that tradecraft is -- is conducting our investigations where we learn more and more about tradecraft. So we try to balance, what do we need to provide to partners so they can best protect themselves, versus not interrupting our investigations if the information were to made -- be made public.
FEINSTEIN: Thank you very much. PRIESTAP: A balancing act.
FEINSTEIN: My time is up. Thank you.
BURR: Thanks, Senator Feinstein.
The Vice-Chairman and I have already decided that we're going to invite the bureau in for a classified briefing to update all members on the open investigations, and any that we see that might warrant, on their minds, an opening of a -- a new investigation.
In addition, let me remind members that one of the -- one of the mandates of -- of our investigation is that we will, at the end of this, work with bureau and other appropriate agencies to make a public report in as graded public detail as we can, our findings on Russia's involvement in our election.
So, it is the intent of the chair, at least, to make sure that as much as we can declassify, it's done and the public gets a -- a true understanding when we put out a final report.
Senator Rubio?
RUBIO: Thank you, Mr. Chairman.
And that's -- that's critically important. I think the most important thing we're going to do in this report is tell the

American people how this happened, so we're prepared for the next time. And what -- it begins, I think, by outlining what their goals were, what they tried to do, in this regard.

And we know what they tried to do, because they've done it in other countries around the world for an extensive period of time. The first is, undermine the credibility of the electoral process. To be able to say, that's not a real democracy. It's filled with all kinds of problems. The second is, to undermine the credibility of our leaders, including the person who may win.

They want that person to go into office hobbled by scandal and all sorts of questions about them. And the third, ideally, in their minds, I imagine, is to be able to control the outcome in some specific instances. If they think they could, either through public messaging, or even in a worst case scenario by actually being able to manipulate the vote -- which I know has now been repeatedly testified did not happen here.

RUBIO: And, by the way, these are not mutually exclusive. You can do all three, you can only take one. They all work in conjunction. I think you can argue that they have achieved quite a bit, if you think about the amount of time that we have been consumed in this country on this important topic and the political fissures that it's developed.

And the way I always kind of point to it -- and if anyone disagrees I want you to tell me this -- but, you know, we have something in American politics. It's legitimate; both sides do it. It's called opposition research. You find out about your opponent. Hopefully it's embarrassing or disqualifying information if you're the opposition research person. You package it. You leak it to a media outlet. They report it. You run ads on it.

Now imagine being able to do that with the power of a nation state, illegally acquiring things like e-mails and being able to weaponize by leaking -- leaking it to somebody who will post that and create all sorts of noise. I think that's certainly one of the capabilities. The other is just straight-out misinformation, right? The ability to find a site that looks like a real news place, have them run a story that isn't true, have your trolls begin to click on that story. It rises on Facebook as a trending topic. People start to read it. By the time they figure out it isn't true, a lot of people think it is.

I remember seeing one in early fall that President Obama had outlawed the Pledge of Allegiance, and I had people texting me about it. And I knew that wasn't true, but my point is that we have people texting about it, asking if it was. It just tells you -- and I don't know if that was part of that effort, or it was just somebody with too much time on their hands.

And then the third, of course, is the access to our voting systems, and obviously people talk about effecting the tallies. But just think about this -- even the news that a hacker from a foreign government could have potentially gotten into the computer system is enough to create the specter of a losing candidate arguing, the election was rigged. The election was rigged.

And -- and because most Americans, including myself, don't fully understand all the technology that's around voting systems per se. You give that "election is rigged" kind of narrative to a troll and a fake news site, and that stuff starts to spread. And before you know it, you have the specter of a political leader in America being sworn in under the cloud of whether or not the election was stolen because vote tallies were actually changed.

So I don't know why they were probing these different systems, because obviously a lot of the information they were looking at was publicly available. You can buy it -- voter roles. Campaigns do it all the time. But I would speculate that one of the reasons potentially is because, they wanted these stories to be out there. That someone had pinged into these systems creating a specter of being able to argue, at some point, that the election was invalid because hackers had touched election systems in key states.

And that is why I really, truly believe, Mr. Chairman, it is so important that, to the extent possible, that part of it, the systems part, as much of it be available to the public as possible. Because the only way to combat misinformation is with truth and with facts, and explain to people, and I know some of it is proprietary. I know some of it we weren't trying to protect methods and so forth, but it is really critical that people have confidence that when they go vote that vote is going to count and someone's not going to come in electronically and

change it.
And I think they're -- I -- I just really hope we err on the side of disclosure about our systems so that people have full confidence that when they go vote.
Because I can tell you, I was on the ballot in November, and I remember people asking me repeatedly, is my vote going to count? I was almost afraid people wouldn't vote because they thought their vote wouldn't count.
So I just hope as we move forward -- I know that's not your decisions to make in terms of declassifications and the like -- but it is really, really, really important that Americans understand how our voting systems work, what happened, what didn't and that -- be able to communicate that in realtime in the midst of an election.
So that if in 2018 these reports start to emerge about our voting systems being pinged again, people aren't -- we can put out enough information in October and early November so people don't have doubts. And I know that's not your decisions to make, but I just really hope that's part of -- of what we push on here, because I think it's critical for our future.
BURR: Senator Wyden.
WYDEN: Thank you, Mr. Chairman.
Let me say to the three of you, and I say it respectfully, that on the big issue, which is which states were affected by Russian hacking in 2016, the American people don't seem to be getting more information than what they already had before they showed up. We want to be sensitive to security concerns, but that question has to be answered sooner rather than later. I want to send that message in the strongest possible way. We obviously need to know about vulnerabilities, so that we can find solutions, and we need better cybersecurity to protect elections from being hacked in the first place. And that means solutions like Oregon's vote-by-mail system, that has a strong paper trail, error-gapped (ph) computers and enough time to fix the problems if they pop up.
But now to my question: You all mentioned the January intelligence assessment, saying that the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying. Your prepared system -- your prepared testimony today makes another point that I think that is important. You say it is likely that cyber-manipulation of U.S. election systems intended to change the outcome of a national election would be detected. So, that is different what we have heard thus far.
So I have two questions for you, Ms. Manfra, and you, Dr. Liles: What level of confidence does the department have in its assessment that 2016 vote tallying was not targeted or compromised? And second, does that assessment apply to state and local elections?
LILES: Thank you, sir, for the question.
So, the level of effort and scale acquired to change the outcome of a national election would make it nearly impossible to avoid detection. This assessment's based on the diversity of systems, the need for physical access to compromise voting machines themselves, the security of pre-election testing employed by the state and local officials. There's a level -- a number of standards and security protocols that are put in place. There's a -- addition, the vast majority of localities engage in logic and accuracy testing, which work to insure voting machines are operating and tabulating as expected.
Before, during, and after the election, there has been an immense amount of media applied to this, which also brings in the idea of people actually watching in and making sure that the election results represent what they see. And plus there's just this statistical anomalies that would be detected, so we have a very high confidence in our assessments.
WYDEN: What about state and local elections? Do you have the same level of confidence?
LILES: So, from the standpoint of a nation-state actor operating against a state and local election system, we would have the same -- for an Internet-connected system, we would have the same level of confidence.
WYDEN: Ms. Manfra?
MANFRA: Yes, sir.
And I think this also gets to Senator Rubio's point about the difficulty in the general public understanding the

variety of systems that are used in our election process.
MANFRA: And so, we broke our level of engagement and concern down a couple of different areas. The voter registration systems, which are often -- can -- usually connected to the internet. We also were looking at the voting machines themselves, which, by best practice and by the voluntary voting standards and guidelines that the Department of Commerce works with the Election Assistance Commission on, is, by best practice -- those are not connected to the internet.
WYDEN: So can Homeland Security assure the public that the Department would be able to detect an attempted attack on vote tallying?
MANFRA: What I would suggest, sir, is that the ability, as has been demonstrated by security researchers, to access remotely, a voting machine to manipulate that vote, and then to be able to scale that across multiple different voting machines made by different vendors, would be virtually impossible to occur in an undetected way within our current election system.
WYDEN: Has the department conducted any kind of post-election forensics on the voting machines that were used in 2016?
MANFRA: We are currently engaged with many vendors of those systems to look into conducting some joint forensics with them. The vendor community is very interested in engaging with us. We have not conducted...
(CROSSTALK)
WYDEN: So there's no -- there's been no analysis yet?
MANFRA: We have not -- our department has not conducted forensics on specific voting machines.
WYDEN: Do you believe it's important to do that? In terms of being able to reassure Americans that there was no attack on vote tallying?
MANFRA: Sir, I would say that we do currently have voluntary standards in place that vendors are enabled -- and in approximately 35 states, actually require, some level of certification of those voting machines that they are complying with those standards. We would absolutely be interested in working with vendors to conduct that level of analysis.
WYDEN: Let me ask one last question. Obviously, the integrity of elections depends on a lot of people. State and local election officers, equipment vendors, third party contractors.
Are you all, at Homeland Security and the FBI, confident that the federal government has now identified all of the potential government and private sector targets?
MANFRA: Yes, sir. I'm confident that we've identified the potential targets.
WYDEN: OK.
Thank you, Mr. Chairman.
BURR: Senator Collins?
COLLINS: Mr. Priestap, let me start by saying that it's a great pleasure to see you here again. I remember back in 2003, you were detailed to the Homeland Security Committee when I was the chairman and how helpful you were in our drafting the Intelligence Reform and Terrorism Prevention Act. So, thank you for your continued public service.
You testified this morning and answered the question of, what does Russia want? And you said that the Russians want to undermine the legitimacy of our elections and sow the seeds of doubt among the American public.
Despite the exposure and the publicity given to the Russian's efforts in this regard, do you have any doubt at all that the Russians will continue their activities in subsequent elections?
PRIESTAP: I have no doubt. I just can't -- I just don't know the scale on aggressiveness, whether they'll repeat that, if it'll be less or if it'll be more. But I have no doubt they will continue.
COLLINS: Is there any evidence that the Russians have implanted malware or backdoors or other computer techniques to allow them the easier access next time to our election systems?

PRIESTAP: I'm sorry, Senator. I just can't comment on that because of our impending investigations.
COLLINS: Secretary Manfra, the secretaries of state who are responsible for the election systems have a pretty blistering attack on the Department of Homeland Security, in the testimonies that will be given later this morning. And I want to read you part of that and have you respond.
They say, yet nearly six months after the designation -- and they mean the designation of election systems as critical infrastructure -- and in spite of comments by DHS, that they are rushing to establish election protections. No secretary of state is currently authorized to receive classified threat information that would help them to protect their election systems. Why not?
MANFRA: Thank you, ma'am, for that question. I would note that this community -- the secretaries of state, and for those states where they have a state election director, is not one that the department has historically engaged with. And what we have done in the process of building the trust and learning about how they do their work and how we can assist, we have identified the need to provide clearances to that community. And so we have committed to them to work through that process between our department and the FBI.
COLLINS: Let me ask you about your own agency, which is the agency that focuses on critical infrastructure, including our election systems. Now, NPPD is not an official element of the intelligence community that would have routine access to especially sensitive classified information.
So how do you know with any certainty whether you and others in the agency are read into all the relevant classified information that may exist regarding foreign threats to our critical infrastructure, including our election system?
MANFRA: Yes, ma'am. I would say, despite the fact that we're not a part of the intelligence community -- and our focus is on network defense and operations, in partnership with the critical infrastructure and the federal government -- we feel very confident that with the partnership with our own intelligence and analysis division, that serves as an advocate for us within the intelligence community, as well as our direct relationships with many of those individuals in organizations such as the FBI, NSA and others, that we receive information quickly. And when we ask to declassify that, there are responses, and we work through our partners at the intelligence analysis office to ensure that that happens quickly. So is there room for improvement? Absolutely, of course, but we have the full commitment of the intelligence community to support us and get us the information that we need and our stakeholders need.
COLLINS: And, finally, how many states have implemented all the best practices recommended in the document developed by DHS regarding the protection of election systems?
MANFRA: Ma'am, I'd have to get back to you on a specific number of states. I don't have them.
COLLINS: Do you think most states have?
MANFRA: In our informal engagement, many of them noted that they had already adopted some of these and to the extent that they weren't -- they were incorporating them.
COLLINS: I would ask for a response for the record.
MANFRA: Yes, ma'am.
COLLINS: That's a really important point.
BURR: Senator Heinrich?
HEINRICH: Mr. Priestap, I want to thank you for just how seriously you've taken this and how you've answered the questions this morning in your testimony. I think you hit the nail on the head when you said we need to step back and ask the fundamental question, what do the Russians want?
And by outlining that they want to undermine legitimacy in our system, that they want to sow discord, that they want to undermine our free and fair elections, we really have a better lens with which to understand the -- the specifics of what happened in 2016. In -- in your view, were the Russians successful at reaching their goals in their activities in our 2016 elections?
PRIESTAP: I don't know for certain whether the Russians would consider themselves successful. In many

ways, they -- they might argue that because of the time and energy we're spending on this topic, maybe it's distracting us from other things. But, on the other hand, exactly what this committee is doing as far as raising awareness of their activities, their aims, for the American people, to me they've done -- in my opinion, they've done the American public a service in that regard. And so, I guess I don't know but could argue either way.
HEINRICH: Yes. I -- I think the -- the jury's certainly out for the future, but when you look at the amount of discord that was sown and the impact on 2016, I hope that the outcome of what we're doing here is to make sure that in 2018, and in 2020, and 2022, that by no metric will they have been successful.
Mr. Priestap, you stated, very correctly, that one of their primary goals was to delegitimize our democracy. Are -- are you familiar with the term unwitting agent?
PRIESTAP: Yes, I am.
HEINRICH: Can you kind of summarize what that is for us?
PRIESTAP: In an intelligence context, it would be where an intelligence service is trying to advance certain names and they reach out to a variety of people, some of which they might try to convince to do certain things. And the -- the people, person or persons they contact might actually carry those out, but for different reasons than the intelligence service that actually wanted them to carry them out. In other words, they do it unwittingly.
HEINRICH: By effectively reinforcing the Russian narrative and -- and publicly saying that our system is rigged, did then candidate Trump -- now President Trump, become, what intelligence officials call, an unwitting agent?
PRIESTAP: I -- I can't give you a comment on that.
HEINRICH: I -- I don't blame you for not answering that question. We've got about a minute 46 left. Can you talk about the relationship between the election penetration that we saw and the coincident Russian use of, what Senator Rubio very aptly described, of trolls, of bots, of social media, all designed to manipulate the American media cycle and how those two things fit together?
PRIESTAP: I'm sorry. To clarify, fit together the intrusions with the...
(CROSSTALK)
HEINRICH: What's the relationship between what they were doing in our elections, from a technical point of view, and what they were seeking to do in our media cycle, by using trolls, and bots and manipulation to the media cycles.
PRIESTAP: The -- the -- I guess the best way I can describe it is that this was a, my opinion, a well planned, well coordinated, multi-faceted attack on -- on our election process and democracy. And, while that might sound complicated, it was actually really straight forward. They want to collect intelligence from a variety of sources, human and cyber means.
They want to evaluate that intelligence, and then they want to selectively -- they might selectively disseminate some of it. They might use others for more strategic discussions, but at the end of the day, it's all about collecting intelligence that would give them some type of advantage over the United States and/or attempt to influence things. And then, coordinated -- well coordinated, well funded, diverse ways to disseminate things to hopefully influence American opinion.
HEINRICH: This is a very sophisticated, highly resourced...
(CROSSTALK)
PRIESTAP: Absolutely.
HEINRICH: Thank you.
BURR: Senator Blunt?
BLUNT: Thank you. Thank you, Chairman.
Let's talk a little bit about once -- let's start with a comment that DHS made in it's written comment which -- which says, in excess, that the systems Russian actors targeted or compromised were not involved in vote tallying. Now is that because the vote tallying systems are a whole lot harder to get into than the voter registration systems?

MANFRA: I can't make a statement as to why different systems were targeted. What we can assess that is that those vote tallying systems, whether it was the machines or a kiosk that a voter uses at the polling station, or the systems that are used to tally votes, were very difficult to access, and particularly, to access them remotely. And -- and then given the level of observation of -- for vote tallying at every level of the process that adds into, you know, that we would have identified issues there and there were no identified issues. So those two are... (CROSSTALK)

BLUNT: OK. I -- I would think that if you could get into the vote tallying system, and you did want to impact the outcome of an election, obviously, the vote tallying system is the place to do that. And I would also suggest that all of your efforts -- most -- a lot of your efforts should be to continue to do whatever DHS thinks they need to advise. I don't think we should centralize this system to give advice to state and local election officials to be sure that that that vote tallying system is protected at a level above other systems.

You know, the voter registration system is public information. It is generally accessible in lots of ways. It's not nearly as protected, for that reason. You have lots of them put from lots of sources into that system. And I think, Ms. Manfra, you made the point that you said that in a -- the best practice would be to not have the vote tallying system connected in any unnecessary way to the internet. Is that right?

MANFRA: Both the kiosks themselves and vote tallying systems, to not connect them to the internet and to also have, ideally, paper auditing trails as well.

BLUNT: Well, I certainly agree with that. The paper trail is significant and -- and I think more prevalent as people are looking at new systems. But also, I think any kind of third party monitoring, the third -- the first two parties would be the voter and the counting system, just creates another way into the system. So, my advice would be that DHS doesn't want to be in a situation where somehow you're connected to all the voting systems of the country.

And Mr. Liles, I think you said the diversity of our voting system is a great strength of the system. Do you want to comment on that any more?

LILES: Yes, sir. When we were setting it as part of our red teaming activities, we looked at the diversity of the voting system as actually a great strength. And the fact that there were not connected in any one kind of centralized way. So we evaluated that as -- when we were looking at the risk assessment with OCIA, the Office of Cyber Intelligence Analysis -- Infrastructure Analysis, we looked at that as one of the great strengths and our experts at DIC we worked with also said the same thing.

BLUNT: Well, I would hope you'd continue to think about that as one of the great strengths, as you look at this critical infrastructure, because every -- every avenue for federal monitoring is also just one more -- one more avenue for somebody else to figure out how to get into that system.

And again, the voter registration system dramatically different in what it does. All public information accessible, printed out, given to people to use, though you are careful of what information you give and what you don't. But almost all election officials that have this system now, have some way to share that with the public, as a system.

There is no reason to share the security of the vote counting system with the public, or to have it available or accessible. And I would hope that the DHS, or nobody else, decides that you're going to save this system by having more avenues -- more avenues into the system.

MANFRA: Absolutely not, sir. We're fully supportive of the voluntary standards process, and we are engaging with that process with our experts and we continue, again, with the voluntary partnership with the state and local. And we intend to continue that.

BLUNT: Thank you. Thank you, Mr. Chairman.

BURR: Senator King?

KING: Thank you, Mr. Chairman.

Starting with a couple of short questions, Mr. Priestap.

Number one, you've stated this was a very grave threat, that Russia -- the attempts to probe and upset our local election systems. Any doubt it was the Russians?
PRIESTAP: No, sir.
KING: Any doubt that they'll be back?
PRIESTAP: No, sir.
KING: To our DHS witnesses, have the 21 states that you've mentioned, that we know where we had this happen, been notified officially?
MANFRA: Sir, the owners of the systems within those 21 states have been notified.
KING: How about the election officials in those states?
MANFRA: We are working to ensure that election officials as well understand. I'll have to get back to you on whether all 21 states...
(CROSSTALK)
KING: Have you had a conference of all state election officials, secretaries of state here in Washington on this issue?
MANFRA: I have had at least two teleconferences, and in-person conferences -- we will be engaging with them in July, I believe.
KING: Well, I would urge you to put some urgency on this. We've got another election coming in 18 months and if we're talking about systems and registration rules, the time is going by. So, I believe, this is -- as we've already heard characterized, is a very grave threat. It's going to be back and shame on us if we're not prepared.
MANFRA: Yes, sir. We have biweekly -- every other week, we hold a teleconference with all relevant election officials, the national associations that represent those individuals have nominated bipartisan individuals to engage with us on a regular basis.
This is of the utmost urgency for the department and this government to ensure that we have better protections going forward. But the community -- the election community is similarly committed and has been so for years.
KING: And just to be clear, nobody's talking about a federal takeover of local election systems or the federal rules. What we're talking about is technical assistance in information and perhaps some funding, at some point.
MANFRA: Sir, this is similar to our engagement with all critical infrastructure sectors, whether it's the electrical sector, the nuclear sector, the financial sector, is completely voluntary, and it is about this department providing information, both to potential victims, but to all network defenders, to ensure that they have access to what we have access to and can better defend themselves.
KING: Thank you.
Mr. Liles, I'll take issue with something that you said -- that we have a national election and it was just too large, too diverse, to really crack. We don't have a national election. What we have are 50 state elections. And each election in the states can depend upon a certain number of counties.
There are probably 500 people within the sound of my voice who could tell you which ten counties in the United States will determine the next presidential election. And so you really -- a sophisticated actor could hack a presidential election, simply by focusing on particular counties. Senator Rubio, I'm sure, remembers Dade County in the year 2000 and the significance that had to determining who the next president of the United States was.
So, I don't think it works to just say, oh, it's a big system and the very diversity will protect us because it really is county by county, city by city, state by state and a sophisticated actor, which the Russians are, could easily determine where to direct their attack. So I don't want to rely on the diversity.
Second -- a separate point is, what do we recommend? And we've talked about paper backups. The Dutch just had an election where they just decided to make it all paper and count the ballots by hand, for this very reason. So what would you tell my elections clerk in Brunswick, Maine, Ms. Manfra, would be the top three things he or she should think about in protecting themselves in this situation?

MANFRA: Sir, I would say, to first, as previous senators mentioned, prioritize the security of your voting machines and the vote tallying system, ensure that they are not connected to the internet -- even if that is enabled on those particular devices.

Second, ensure that you have an auditing process in place where you can identify anomalies throughout the process, educate polling workers to look for suspicious activity, for example.

KING: But does -- doesn't auditing mean a paper trail, a paper backup?

MANFRA: Yes, sir. I would recommend a paper backup.

KING: And one of the worrisome things, again, on the issue of the national, we talk about how diverse it is, but aren't we seeing a consolidation in terms of the vendors who are producing these machines? MANFRA: Yes, sir. It is my understanding that we are seeing some consolidation in the vendor community. Again, many of them are committed and have engaged on the voluntary voting standards and guidelines, which partly include security.

We will be updating those security guidelines in 2018, and yes, while there is some concern about consolidation, we do look forward to engaging with them, and as of now, they are a very engaged community.

KING: I think this aspect of this question that we're -- this committee is looking at is one of the most important, and frankly, one of the most daunting, because we pretty well determined that they weren't successful in changing tallies and changing votes but they weren't doing what they did, in at least 21 states, for fun.

And they are going to be back, and they're going to be back with knowledge and information that they didn't have before. So I commend you for your attention to this and certainly hope that this is treated with the absolute utmost urgency.

KING: Thank you, Mr. Chairman.

BURR: Senator Lankford?

LANKFORD: Thank you, Mr. Chairman.

Thanks to all of you for being here as well today.

So, Senator King, just as a heads up, there are some states that are like that. For 25 years the Oklahoma election system has had a paper ballot, and an optical scan and it's been a very good back-up for us. We -- we quickly count because of the optical scan, but we're able to go back and verify because of paper.

This is such a big deal and it's such an ongoing conversation that I'm actually in two simultaneous hearings today, I'm running back and forth with. In the Department of Homeland Security, and what we're dealing with with state elections, and with state systems, is also happening in the HSGAC hearing that I'm also at, including my own Oklahoma CIO that's there testifying today, on this same issue.

How we are protecting state systems, state elections and what's happening? I brought this with me today, you all are probably -- this group is very, very familiar with this e-mail. This is the famous e- mail that Billy Rinehart got, from the DNC, while he happened to be on vacation. He was out in Hawaii enjoying some quality time away from his work at the DNC, and he gets a -- an e-mail from Google, it appears, that says someone has used your password, someone just tried to sign-in to your Google account.

Sent it to him and told him someone tried to do it from the Ukraine, and recommended that he go in and change his password immediately. Which, as the New York Times reported, he groggily at 4 a.m., when he saw that e-mail was frustrated by it, went in, clicked on the link, changed his password and went back to bed.

But what he actually did, was just gave the Russian government access to the DNC, and then it took off from there. Multiple other staff members of the DNC got an e-mail that looked just like this. Now, for everyone who has a Google account, will know that really looks like a Google account warning.

It looked like the real thing when you hovered over the changed password, it showed a Google account connection, where it was going to, but it wasn't. It was going to the Russians. About 91 percent, my understanding is, about 91 percent of the hacks that come into different systems, start with a spear phish attack that looks just like this.

So let's -- let's talk about, in practical terms, for our state election folks and what happens in my state and other states. First, for you, Mr. Priestap, how does Russia identify a potential target? Because this is not just a random e-mail that came to him, this was targeted directly at him, to his address. It looked very real, because they knew who he was and where he works. So, how were the Russians that savvy to be able to track this person and how does this work in the future for an election system for a state?

PRIESTAP: So I can't go into great detail in this forum, but I'd say what intelligent services do, not just Russia there, is they're looking for vulnerabilities. That -- that would begin in the cyber sense with computer vulnerabilities. As far as targeting specific individuals, I -- I don't know all the facts surrounding that e-mail and all the e-mails were sent, but my guess is, they didn't just send it to one person. They send it -- sent it the e-mail like that to a whole variety of -- just hoping that one would click on it.

LANKFORD: Right. But how are they getting that information? Are they going to their -- their website, for instance, and gathering all the e-mails for it? I'm trying to figure out, are they tracking individuals to get more information, so they get something that looks like something they would click on?

PRIESTAP: Yes. You hit on it, but a whole variety of ways. They might get it through reviewing open source material, either online or otherwise, but they also collect a lot of information through their -- through human means.

LANKFORD: So, Ms. Manfra, let me ask you this question. When someone, at any location, clicks on a link like this, what access to information do they get typically?

MANFRA: Well, sir, it depends on -- on the system itself. I -- I imagine that's probably a frustrating response, but given the -- and I think this is important for the public to understand, is, as the -- the threat evolves they're going to continue as we educate the public, don't click on certain things. Look at, you know, make sure you know the sender, for instance before you click on it and as our defense gets better the offense is going to look for other means.

And so we look, you know, in this case, ideally, we want people to look and see what -- what is it that they're actually clicking on before they click it. Some organization to -- to say when an individual clicks on that link, they choose to not allow that to go to that destination, because they know it's suspicious or they have some mechanisms in place to put that into a container and look at it. Other organizations don't take those steps and it really depends on your risk management and the technical control that you put in place.

LANKFORD: Let me ask you a quick question. Who has primary responsibility for Federal election integrity? Which agency is the prime mover in that? Obviously, states oversee their own, but which Federal entity is working with the state to say they're the prime person -- or the prime agency to do it? MANFRA: For election cybersecurity, our -- our department, in coordination with the FBI and others, is leading the partnership with state and locals.

LANKFORD: Great. Thank you.

BURR: Senator Manchin?

MANCHIN: Thank you, Mr. Chairman.

And thank all of you for your appearance here today and your testimony. Being a former Secretary of state of the -- my great state of West Virginia, and also being a former governor, my utmost concern was voter fraud. Every time that we would have a report of a fraud, I would see the election participation decrease, the next election cycle, thinking their vote didn't count.

Is there any reason, at all, that any person that has the knowledge that you all have, or anyone that you've -- on our committee here, from the intelligence community, would give you any doubt that Russia was involved, and Russia was very much involved with the intent of doing harm to our election process, as far as the confidence level that voters would have? Do any of you have any concerns, whatsoever, any doubts, that the Russians were behind this and involved in a higher level than ever? All three of you.

PRIESTAP: No -- no doubt from the FBI's end as far as the -- as far as Russia's involvement.

MANCHIN: And you've all interacted with all the intelligence community right?
PRIESTAP: Yes, sir.
MANFRA: Similar, sir. I have no doubt.
MANCHIN : There's not an American right now that should have a reasonable doubt whatsoever that the Russians were involved? Were all 50 states notified on Russia's intentions and activities during the '20 (sic) election cycle? Had you all put an alert out? So if I'd have been secretary of state in charge of my elections in West Virginia, would you have notified me to be on the lookout?
MANFRA: Sir, I can discuss our products that we put out and I'll defer to the FBI on -- on what they put out. We did put out products, not public products, but we did put out products, primarily leveraging our multi-state information sharing analysis center, which has connections to all 50 states CIOs.
And we engaged with the Election Assistance Commission and other national associations that represent those individuals to ensure that we were able to reach, again this was a community that we had not historically engaged with, and so, we relied on those, that we did put out multiple products prior to the election.
MANCHIN: And you're really not sure if these national associations, like (ph) the secretary of states, dispersed that information, put everybody on high alert?
MANFRA: I -- I believe that they did, sir. We also held a conference call, where all 50 secretaries of state, or an election director, if the -- if the secretary of state didn't have that responsibility. In August, and September and again in October, both high level engagement and network defense products.
MANCHIN: And if I could ask this questions to whoever, maybe Mr. Priestap, what was Russia's intention, and do you think they were successful in what they desired to do, even thought they didn't alter -- as you all have said, you can see no alterations of the election results. Do you believe that it had an effect in this election outcome -- in the outcome of this 2016 election?
PRIESTAP: As far as Russia's intention, again, the broader being to undermine democracy and one of the ways they sought to do this, of course, here, was to undermine the legitimacy of our free and fair election.
MANCHIN: Do you believe they were successful in the outcome?
PRIESTAP: No, I -- the FBI doesn't look at that, as far as, did Russia achieve its aims in that regard.
MANCHIN: Let me ask this question. Are there counter actions the U.S. can take to subvert or punish the Russians for what they have done, and their intention to continue? And what's your opinion of the sanctions that we have placed on Russia?
PRIESTAP: Sure. As you know, the FBI doesn't do policy. I'm here today to provide you an overview of the threat picture, at least, as I understand and see it. But obviously the U.S. government did take action post-election in regards to making a number of Russian officials...
(CROSSTALK)
MANCHIN: Have you seen them subside, at all, any of their activities since we have taken some actions?
PRIESTAP: Subside? They have less people to carry out their activities, so it's certainly had an impact on the number of people.
MANCHIN: And finally, with the few seconds I have left, have we shared this with our allies, our European allies, who are going through election processes and have they seen the same intervention in their election process that we have seen from the Russians in ours? PRIESTAP: Sure. I can't speak for DHS, but the FBI is sharing this information with our allies, absolutely.
MANCHIN: How about DHS?
MANFRA: We are also sharing information with our allies.
MANCHIN: Are they seeing a high -- an overaggressive, high activity, from the Russians that they haven't seen at this level before, such as we did during the 2016 election?
LILES: Sir, there is immediate reporting that suggests that. We don't have direct government-to-government relationships from a DHS perspective. There is definitely immediate reporting that they're seeing an increased

activity.
MANCHIN: Thank you.
BURR: Senator Cotton?
COTTON: Thank you all for your appearance today.
Mr. Priestap, in response to Mr. Heinrich's question about whether Donald Trump had become an unwitting agent of Russia, and their efforts to sow discord and discontent about our elections, you said that you decline to answer, which is understandable.
Let's look at this from a different perspective. Since her election defeat, Hillary Clinton has blamed her loss on the Russians, Vladmir Putin, the FBI, Jim Comey, fake news, Wikileaks, Twitter, Facebook and my personal favorite, content farms in Macedonia. In her blaming her loss on these actors, has Hillary Clinton become an unwitting agent of Russian's goals in the United States?
PRIESTAP: And I'm sorry, sir, but I'd rather not comment. It's just something...
(CROSSTALK)
COTTON: I understand. I just wanted to point out that you can look at it from two different...
(CROSSTALK)
PRIESTAP: ...it's just something I haven't given any thoughts to.
COTTON: Let's turn to other matters, then. Would you advise states and localities in the conduct of their elections, or more broadly, in their government services, not to use, or not to do business with Kaspersky Labs, companies that do business with Kaspersky or companies that use Kaspersky products in their systems?
PRIESTAP: Sir, I can't really comment on that in this setting.
COTTON: Miss Manfra, would you advise them not to use Kaspersky products?
MANFRA: I also cannot comment on that in this forum, sir.
COTTON: I don't even have to ask, Dr. Liles. You're reaching for your microphone.
LILES: Yes, sir. I can't comment either.
COTTON: OK. Senator Risch says he'll answer, but I'll let him speak for himself at a later time. Mr. Priestap, we've talked a lot about Russia's intent and activities in our elections but I think it's important that the American people realize that it goes much farther than just elections and the 2016 campaign, as well.
Isn't it true that Russian cyber actors have been probing U.S. critical infrastructure for years?
PRIESTAP: Yes, sir. I can't go into specifics but they probe a lot of things of critical importance to this country.
COTTON: And as the head of counter intelligence, you write in your statement, that quote, "Russia's 2016 presidential election influence effort was its boldest, to date, in the United States" which implies there have been previous efforts. You also say that the FBI had to strengthen the intelligence community assessment because of our history investigating Russia's intelligence operations within the United States. Both of which suggest that this keeps you pretty busy in your portfolio and counterintelligence, is that right?
PRIESTAP: That's correct.
COTTON: And this is -- Russian intelligence threat is not just a cyber threat either. It also is a threat from traditional human intelligence, or what a layman might call spies, is that right?
PRIESTAP: Yes, sir.
COTTON: Do so called diplomats who work down at the Russian embassy in Washington D.C. have a requirement to notify our state department in advance if they plan to travel more than 25 miles, and give that notification 48 hours in advance?
PRIESTAP: They do.
COTTON: And the State Department's supposed to notify the FBI in advance of those travel arrangements, correct?
PRIESTAP: Yes.
COTTON: Is it true that the Russian nationals often fail to give that notification, at all, or they give it at, say, 4:55

on a Friday afternoon before a weekend trip?
PRIESTAP: I'd prefer not to go into those details here, but -- I'll leave it at that. COTTON: Does it complicate you and your agents' efforts to conduct your counterintelligence mission, to have Russian nationals wandering around the country more than 25 miles outside their duty assignment?
PRIESTAP: Sure. If that were to happen, that would absolutely complicate our efforts.
COTTON: The Secretary of Defense recently indicated, at a Armed Services Committee hearing, that Russia is in violation of something called the Open Skies Treaty, a treaty we have with Russia and other nations that allow us to overfly their territory and take pictures and they do the same here. Do we see so called Russian diplomats traveling to places that are in conjunction with open skies flights that Russia's conducting in this country?
PRIESTAP: I'm sorry, I just can't comment on that here.
COTTON: OK. Is it -- so last summer, a American diplomat in Moscow was brutally assaulted on the doorstep of our embassy in Moscow. Did we take any steps to retaliate against Russia for that assault in Moscow? Did we declare persona non grata any of their so called diplomats here in the United States?
PRIESTAP: If I recall correctly, we didn't immediately do anything in that regard.
COTTON: OK. This committee passed, unanimously, in committee last year, something that just passed as part of the (inaudible) in April a provision that would require one, the State Department to notify the FBI of any requests for Russian diplomats to travel outside their embassy and to report violations to you.
It further requires the State Department to report those violations, regularly, to this committee. What's the status of that provision, now that it's been in law for about two months? Is the State Department cooperating more fully with you?
PRIESTAP: I guess I'd rather not comment on that here. We're still working through the implementation of that.
COTTON: Well, I certainly hope they start. Thank you.
BURR: Senator Harris?
HARRIS: Thank you. Ms. Manfra, you mentioned that you notified the owners. I'm not clear on who the owners are. Are they the vendors?
MANFRA: What I meant to clarify is, in some case, it may not be the secretary of state or the state election director who owns that particular system, so in some cases it could be a locality or a vendor.
HARRIS: So is there a policy of who should be notified when you suspect that there's a threat?
MANFRA: We are working through that policy with the secretaries of state, that is one of the commitments that we made to them, as election directors, in order to ensure that they have appropriate information, while preserving the confidentiality of the victim, publicly.
HARRIS: And can you tell us which states - in which states you notified the vendor instead of notifying the secretary of state?
MANFRA: We keep the vendor information confidential as well.
HARRIS: Are there states that you notified where you did not notify the person who was elected, by the people of that state, to oversee elections?
MANFRA: I don't believe that's the case but I will get back to you with a definitive answer.
HARRIS: And how specific was the warning that you sent? What exactly is it that you notified the states or the vendors of?
MANFRA: Depending on the scenario, and the information that we had, and more generally what we do, is when we get classified information, we look to declassify as much as possible to enable...
(CROSSTALK)
HARRIS: Let's talk about the election, yeah.
MANFRA: So for this particular one, what we took was technical information that we had, that we believed was suspicious, and that was emanating from Russia, and was targeting their system, we asked them to look at their

system. We asked, and this was part of the broader dissemination, as well, we asked all states to look at their system, to indentify whether they had an intrusion, or whether they blocked it. In most cases, they blocked it.
HARRIS: Do you have a copy with you of the notification you sent to these various vendors or states?
MANFRA: I do not, ma'am, but we can get back to you.
HARRIS: OK, and will you provide this committee with a copy of the notification you sent to those states or vendors?
MANFRA: Many of them were done in person, but what I can show you is the technical information. That was also rolled up in the information that we published in December, but I can show you what we provided to the states and localities.
HARRIS: And did you notify each of them the same way? Or did you tailor the notification to each state?
MANFRA: We tailor the notification. It's a process for all victim, or potential victim, notification -- us and the FBI, so sometimes it may be an FBI field agent that goes out there, sometimes it may be a department official that goes out there.
HARRIS: OK, so in your follow-up to the committee, please provide us with, specifically, who notified each state, and then who in that state was notified, the vendor or the state election official, and also what specifically they were notified of. I have, in 2007, California worked with leading security researchers, the secretary of state at the time was Deborah Bowen, and they instituted some of the best practices, we believe, for election security. And my understanding is that it is considered a gold standard. So my question is, does DHS have the technical capability and authority to coordinate a study like that for all of the states?
MANFRA: We do have the technical capability and authority to conduct those sorts of studies, ma'am, yes.
HARRIS: Have you pursued that as a viable option to help the states do everything they can to secure their system?
MANFRA: That is one of the areas that we're considering, yes, ma'am.
HARRIS: So have you taken a look at that study that was commissioned in California, in 2007? And if not, I'd encourage that you do.
MANFRA: I have not personally, but I will read it, ma'am.
HARRIS: And I'm also concerned that the federal government does not have all the information it needs in these situations where there's been a breach. Is there any requirement that a state notify the federal government when they suspect there's been a breach?
MANFRA: No, ma'am.
HARRIS: And in terms of the American public and voters in each of these states, can you tell me is there any requirement that the state notify its residents when the state suspects there may be a breach?
MANFRA: I cannot comment. I know that multiple states have different sunshine laws, et cetera, that apply to data breaches within the state, so I couldn't make a general statement about what their requirements are at the state level.
HARRIS: And do any of you have any thoughts about whether there should be such requirements, both in terms of states reporting to the federal government, and also states reporting to their own residents and citizens about any breaches of their election system?
MANFRA: Required data breach reporting is a complicated area. We prefer, and we've had a fair amount of success with, voluntary reporting and partnerships, but we'd be happy to work with your staff in further understanding how that might apply here.
HARRIS: OK, I appreciate that. Any other thoughts, as we think about how we can improve notification and sharing of information? No. OK, thank you.
BURR: Before I move to Senator Reed, let me just say that since a number of members have questioned the agencies, especially those that are here, and the sharing with Congress of the investigation, I'll just say that the Chair and the Vice Chair were briefed at the earliest possible time, and continued to be briefed throughout the

process, and then it was opened up to all the members of the committee. I'm not sure that I had ever shared that with everybody but I just want to make sure that everybody's aware of that.

Senator Reed?

REED: Thanks very much, Mr. Chairman.

Thank you very much, ladies and gentlemen. Let's start with Mr. Priestap. Are you aware of any direction or guidance from President Trump to conduct this investigation about the Russian cruising (ph) in our elections?

PRIESTAP: Sir, I can't comment on that. It could be potentially related to things under the special councils purview.

REED: Thank you.

Ms. Manfra, in terms of home security, are you aware of any direction by the president to conduct these types of operations, or your investigations?

MANFRA: Sir, to clarify the question, direction from the president to...

(CROSSTALK)

REED: The President of the United States has directed that we, the Department of Homeland Security, and other federal agencies conduct a - the activities that you're conducting, essentially investigation, in to Russian hacking in the election.

MANFRA: I can't comment on the president's directions, specifically, but our secretary is committed to understanding what happened, ensuring that we are better protected in the future, so our activities are fully supported.

REED: He has not communicated that this is at the direction of the President of the United States?

MANFRA: No, sir.

REED: Director Liles?

LILES: Sir, this comes directly written down from the IC (ph) who has been working on this for quite a while, and so, and the secretary has completely supported it.

REED: But again, no...

(CROSSTALK)

LILES: Nothing from the president directly, sir.

REED: Thank you. I thought Senator King raised some very interesting issues, in terms of most election - national elections, as much you like to think about it, particularly from Rhode Island, are not decided in certain states, but decided even in certain cities and counties. Which raised an interesting question -- you were very assertive about that you'd be able to diagnose an intrusion that was altering voter -- votes, literally. When could you do that? Within weeks of an election, on Election Day, after Election Day?

LILES: Sir, from an IEC perspective, the way we would do that is by looking at the threats themselves that were targeting specific entities. And the other element that we would look at is, as the reporting itself was coming in, if there was any statistical anomalies we were seeing. And I'd also point out, that we're talking about internet-connected systems here, and not all of the key counties that you would represent would be those internet-connected systems.

REED: But, effectively, like -- I think what you've said is, that you'd really have to wait for confirmation until the results started coming in on election day, which raises the issue of -- even if you detect it on Election Day, what do we do?

The votes have already been cast. Are you -- is anyone planning on -- what's the -- what reaction we take? How do we notify people? What are -- what steps do they take?

LILES: I'd have to defer to other (OFF-MIKE).

MANFRA: Yes, sir. And I do want to clarify, when we say that that activity would be difficult to detect, it would be -- or difficult to go on undetected, it would -- that we're discussing both at the polling station or the jurisdiction -- that it would be hard for somebody to do that without anybody -- not necessarily that the department would --

would have that immediate insight.
And, to answer your question, yes, that is absolutely something that is a part of our planning and -- and what we would look forward to partnering with the state and local officials on understanding.
REED: So we're, again, about 18 months away from election. We have to be able to develop a -- not technical infrastructure, but an organizational infrastructure that could react, maybe on very short notice, to discovery that actual votes were being tampered. Is that accurate?
MANFRA: Absolutely, sir. It is both technical and organizational.
REED: And do you think there's enough emphasis in terms of the resources and support to do that, the collaboration? I -- you've got 50 states, and among those states, many of the voting jurisdictions are not at the state level -- they're the city and town canvasser. Are we taking it serious enough? I guess that's the issue.
MANFRA: Absolutely, sir. This is one of our highest priorities. And I would also note that we're not just looking ahead to 2018, as election officials remind me, routinely, that elections are conducted on a regular basis. And so -- highest priority, sir. Yes.
REED: Let me ask Mr. Priestap, if I've pronounced it incorrectly., forgive me. But you -- you testified today, and your colleagues, that information was exfiltrated by the Russians. What type of information was taken, and what could it be used for?
PRIESTAP: Yes, sir. I don't want to get into the -- the details of which -- what victim information was taken. Again, we've got a variety of pending investigations.
But it -- it -- again, it could be used for a variety of purposes. Could have been taken to understand what's in those systems. It could have been taken to use to try to target -- learn more about individuals, so that they could be targeted.
It could -- it could have been taken in a way to then publicize, just to send a message, that a foreign adversary has the -- ability to take things and to sow doubt in our voters' minds.
REED: Let me ask you this question, as a judgment. Given the activities that the Russians have deployed, significant resources, constant effort over -- as you -- the intelligence community -- probably a decade, do you think they have a better grasp of the vulnerabilities of the American voting system than you have?
PRIESTAP: I hope not. I think it's a -- I think it's an excellent question and I can -- well, first of all, I hope not and I don't think so, but if they did, I don't think they do anymore.
REED: Thank you very much.
BURR: Thank you, Senator Reed.
Before we move to the second panel, one last question, Mr. Priestap, for you.
Is there any evidence that the attempt to penetrate the DNC was for the purposes of launching this election year intrusion process that they went on? Or was this at the time one of multiple fishing expeditions that existed by Russian actors in the United States?
PRIESTAP: In my opinion, it was one of many efforts. You'd call it a fishing expedition, but to determine again, what's out there, what intelligence can they collect. So they don't go after one place. They go after lots of places and then...
BURR: Tens? Hundreds? Thousands?
PRIESTAP: Hundreds. . At least hundreds.
BURR: OK.
I want to wrap up the first panel with just a slight recap.
I think you have thoroughly covered that there's no question that Russia carried out attacks on state election systems. No vote tallies were affected or affected the outcome of the elections. Russia continues to engage in exploitation of the U.S. elections process and elections are now considered a critical infrastructure, which is extremely important and does bring some interesting potential new guidelines that might apply to other areas of critical infrastructure that we have not thought of because of the autonomy of each individual state and the

control within their state of their election systems.
So I'm sure this will be further discussed as the appropriate committees talk about federal jurisdiction, where that extends to. And clearly, I think it's this committee's responsibility as we wrap up our investigation to hand off to that committee somewhat of a road map from what we've learned or areas that we need to address, and we will work very closely with DHS and with the bureau as we do that.
With that, I will dismiss the first panel and call up the second panel.
END

Subject: Intelligence gathering; Committees; Local elections; State elections; Presidential elections; National security; Democracy; Politics;

Location: Russia United States--US

Company / organization: Name: Federal Bureau of Investigation--FBI; NAICS: 922120;

Publication title: Political Transcript Wire; Lanham

Publication year: 2017

Publication date: Jun 21, 2017

Publisher: CQ Roll Call

Place of publication: Lanham

Country of publication: United States

Publication subject: Political Science

Source type: Wire Feeds

Language of publication: English

Document type: News

ProQuest document ID: 1912737473

Document URL: https://search.proquest.com/docview/1912737473?accountid=14026

Copyright: 2017 Bloomberg Government

Last updated: 2017-06-23

Database: Global Newsstream,ABI/INFORM Trade & Industry

Contact ProQuest
Copyright © 2017 ProQuest LLC. All rights reserved. - Terms and Conditions

Exhibit 32

Report Information from ProQuest

July 12 2017 17:47

18-F-1517//1061

Table of contents

18-F-1517//1062

S INTEL HEARING ON RUSSIAN INTERFERENCE IN 2016 ELECTION, PANEL 2

Publication info: Political Transcript Wire ; Lanham [Lanham]21 June 2017.

ProQuest document link

Links: Check SFX for Availability

Full text: S Intel Hearing on Russian Interference in 2016 Election, Panel 2

JUNE 21, 2017

SPEAKERS: SEN. RICHARD M. BURR, R-N.C. CHAIRMAN SEN. JIM RISCH, R-IDAHO SEN. MARCO RUBIO, R-FLA. SEN. SUSAN COLLINS, R-MAINE SEN. ROY BLUNT, R-MO. SEN. TOM COTTON, R-ARK. SEN. JAMES LANKFORD, R-OKLA. SEN. JOHN CORNYN, R-TEXAS SEN. MARK WARNER, D-VA. VICE CHAIRMAN SEN. RON WYDEN, D-ORE. SEN. MARTIN HEINRICH, D-N.M. SEN. JOE MANCHIN III, D-W.VA. SEN. KAMALA HARRIS, D-CALIF. SEN. DIANNE FEINSTEIN, D-CALIF.

SEN. ANGUS KING, I-MAINE

WITNESSES: CONNIE LAWSON, INDIANA SECRETARY OF STATE, PRESIDENT-ELECT, NATIONAL ASSOCIATION OF SECRETARIES OF STATE

MICHAEL HAAS, MIDWEST REGIONAL REPRESENTATIVE, NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS

J. ALEX HALDERMAN, PROFESSOR OF COMPUTER SCIENCE AND ENGINEERING, UNIVERSITY OF MICHIGAN

STEVE SANDVOSS, EXECUTIVE DIRECTOR, ILLINOIS STATE BOARD OF ELECTIONS

[*] BURR: I now call the second panel to order, and ask those visitors to please take their seats. As we move into our second panel this morning, our hearing is shifting from a federal government focus to a state-level focus. During this second panel, we'll again -- we'll gain insight into the experiences of the states in 2016, as well as hear about efforts to maintain election security moving forward.

For our second panel, I'd like to welcome our witnesses: the Honorable Connie Lawson, president-elect of the National Association of Secretaries of State and the secretary of state of Indiana; Michael Haas, the Midwest regional representative to the National Association of State Election Directors and the administrator of the Wisconsin Election Commission; Steve Sandvoss, executive director of the Illinois State Board of Elections; and Dr. J. Alex Halderman, professor of computer science and engineering, University of Michigan.

Thank you all for being here.

Collectively, you bring a wealth of knowledge and a depth of understanding of our state election systems, potential vulnerabilities of our voting process and procedures and the mitigation measures we need to take at the state level to protect the foundation of American democracy.

In January of this year, then-Secretary of State -- Secretary of Homeland Security Jeh Johnson designated the election infrastructure used in federal elections as a component of U.S. critical infrastructure. DHS stated that the designation of established election infrastructure as a priority within the national infrastructure protection plan.

It enabled the department to prioritize out cybersecurity assistance to state and local election officials for those who requested, it and made it publicly known that the election infrastructure enjoys all the benefits and protections of critical infrastructure that the U.S. government has to offer.

Some of your colleagues objected to this designation, seeing it as federal government interference. Today, I'd like to hear your views on this specifically, but more broadly, how the states and the federal government can best work together. I'm a proud defender of states' rights but this could easily be a moment of divided we fall. We must set aside our suspicions and see this for what it is, an opportunity to unite against a common threat.

18-F-1517//1069

Together, we can bring considerable resources to bear and keep the election system safe. Again, I'd like to thank our witnesses for being here.

And at this time, I'd turn to the vice chairman for any comments he might make.

The vice chairman doesn't have any.

I will assume, Mr. Haas, that by some process, you have been elected to go first? Unless there is an agreement -- which -- where are we going to start?

HAAS: Actually, I think we were going to defer to Secretary Lawson to start, if that's OK with the chair.

BURR: Madam Secretary, you are recognized.

LAWSON: Well, good morning, Chairman Burr and Vice Chairman Warner and distinguished members of the committee. I want to thank you for the chance to appear before you today. It's an honor to represent the nation's secretaries of state, 40 of whom serve as chief state election officials.

I am Connie Lawson, Indiana secretary of state and I'm also president-elect of the bipartisan National Association of Secretaries of State. I'm here to discuss our capacity to secure state and locally run elections from very significant and persistent nation- state cyber threats.

With statewide elections in New Jersey and Virginia this year and many more contests to follow in '18, I want to assure you and all Americans that election officials across the United States are taking cybersecurity very seriously.

First and foremost, this hearing offers a chance to separate facts from fiction regarding the '16 presidential election. As noted many times, we have seen no evidence that vote casting or counting was subject to manipulation in any state or locality, nor do we have any reason to question the results. Just a quick summary of what we know about documented foreign targeting of state and local election systems. In the 2016 election cycle, as confirmed by the Department of Homeland Security, no major cyber security issues were reported on Election Day, November 8.

Last summer, our intelligence agencies found that up to 20 state networks had been probed by entities essentially rattling the door knobs to check for unlocked doors. Foreign-based hackers were able to gain access to voter registration systems in Arizona and Illinois, prompting the FBI to warn state election offices to increase their election security measures for the November election. In more recent days, we've learned from a top-secret NSA report that the identity of a company providing voter registration support services in several states was compromised.

Of course, it's gravely concerning that election officials have only recently learned about the threats outlined in the leaked NSA report, especially given the fact that the formed DHS Secretary Jay Johnson repeatedly told my colleagues and I that no specific or credible threats existed in the fall of '16. It is unclear why our intelligence agencies would withhold timely and specific threat information from election officials.

I have every confidence that other panelists will address voting equipment risk and conceptual attack scenarios for you today. But I want to emphasize some systemic safeguards that we have against cyber attackers.

Our system is complex and decentralized with a great deal of agility and low levels of connectivity. Even within states, much diversity can exist from one locality to the next. This autonomy serves as a check on the capabilities of nefarious actors.

I also want to mention the recent designation of election systems as critical infrastructure. Real issues exist with the designation, including a lack of clear parameters around the order which currently provides DHS and other federal agencies with a large amount of unchecked executive authority over our election's process. At no time between August of '16 and January of '17 did NASS and its members have a thorough discussion with DHS on what the designation means.

Threat sharing had been touted as a key justification for the designation. Yet, nearly six months later, no secretary of State is currently authorized to receive classified threat information from our intelligence agencies. From information gaps to knowledge gaps that aren't being addressed, this process threatens to erode public

confidence in the election process as much as any foreign cyber threat. It's also shredding the rights that states hold to determine their own election procedures subject to the acts of Congress. If the designation ultimately reduces diversity and autonomy in our voting process, the potential for adverse effects from perceived or real cyber effects -- attacks, excuse me -- will likely be much greater and no the other way around. Looking ahead, the National Association -- the NASS Election Security Task Force was created to ensure that state election officials are working together to combat threats and foster effective partnerships with the federal government and other public-private stakeholders. In guarding against cyber threats, the trendline is positive, but more can be done. Most notably, many states and localities are working to replace or upgrade their voting equipment.

If I have one major request for you today, other than rescinding the critical infrastructure designation for elections, it is to help election officials get access to classified information sharing. We need this information to defend state elections from foreign interference and respond to threats.

Thank you. And I look forward to answering your questions.

BURR: Thank you, Secretary Lawson. Who would like to -- Mr. Haas?

HASS: Thank you. Good morning.

Chairman Burr, Vice Chairman Warner and committee members, on behalf of the National Association of State Election Directors, thank you for this opportunity to share what states learned from the 2016 elections and some steps that it will be -- we are taking to further secure our election systems. I serve as Wisconsin's chief election official, and I'm a member of NASS at the executive board.

We do not have a state elected official who oversees elections in Wisconsin. Many of our state election directors across the country are housed in the secretary of state's offices, but some are not.

The 2016 president election reinforced several basic lessons, although sometimes in a new context. For instance, all must understand the importance of constant and effective communication to ensure that all actors have the tools they need. The new twist (ph) in 2016 of course involved communicating about the security of election systems with the Department of Homeland Security as well as the state staff who provide cyber security protection to our voter registration databases.

As we have heard this morning, some states have expressed concerns about the timeliness and the details of communications from Homeland Security regarding potential threats -- security threats to state election systems. The recent reports about attempted attacks on state voter registration systems, which occurred last fall, caught many states by surprise.

We look forward to working with DHS and other federal officials to develop protocols and expectations for communicating similar information going forward. For example, state election officials believe it is important that we be in the loop regarding contacts that DHS has with local election officials regarding security threats such as the spear-fishing attempts that were recently publicized. States should be aware of this information to protect their systems and so that we can provide additional training and guidance to local election officials.

I appreciate the concern that was expressed this morning that this is a two-way street. And we, at the state level, need to also think carefully about how -- how to most effectively communicate with our local election officials if and when there is an incident that we are aware of at the state level. As part of the DHS designation of election systems as critical infrastructure, bodies (ph) such as coordinating counsels can help to facilitate decisions regarding the proper balance between notifying state and local officials, and protecting confidential or sensitive information.

NASED believes that those coordinating bodies should consist of a broad representation of stakeholders. And we have expressed our strong interest to DHS in participating on those bodies. I would also note that the executive board of NASED supports the request of the U.S. Elections Assistance Commission that it serves as the co-sector's specific -- specific agency as the logical federal agency to partner with DHS to provide subject matter expertise and assistance in communicating with local election officials as the EAC has that communication structure already in place.

18-F-1517//1069 FOIAQuest

HASS: The 2016 elections also reinforced the need for constantly enhancing the security of voter registration databases, as we have heard this morning. While hacking into a voter registration system has no effect on tabulating election results, intrusions could result in unauthorized parties gaining access to data, regarding voters, candidates, ballot contests, and polling places.

I would note that while much of that information is public upon request, there may be some confidential data held in those databases, such as the voter's date of birth, the driver's license number, the last four digits of the social security number. Different states have different laws about what pieces of that data is confidential.

The 2016 elections demonstrated that state and local election officials can implement steps to improve the -- the security of voter data, and then (ph) many of these steps are not complicated.

In addition to the cyber hygiene scans and risk assessments, states are implementing greater use of multi-factor authentication, for users of our systems, updating firewalls, the use of white list, to block unauthorized users, and completely blocking access from any foreign IP address.

The final lesson of 2016 I would like to address relates to voting equipment. To be clear, as it has been said many times this morning, there is no evidence that voting machines or election results have been altered in U.S. elections.

I appreciate the committee's emphasis on that. I think that for the public that cannot be states enough, and strongly enough. Still, we as election administrators must exercise vigilance to assure that such theoretical attacks do not become reality, and we must also continue to educate the public about safeguards in the system. Those safeguards include the decentralized structure of elections that we've heard about this morning and the diversity of voting equipment.

Also, in most cases voting equipment is not connected to the Internet, and therefore cannot be attacked through cyber space. Also it is important to keep in mind that 3 out of 4 ballots cast in American elections are on paper ballots. Most ballots cast on touch screen equipment also have a paper trail that voters can immediately verify their votes, and then election officials can use for audits, and recounts.

There are also several redundancies in the testing and certification of voting equipment. It's important to realize that voting equipment is not only used on Election Day. It's functionality is tested several times during the process.

In short, the 2016 election's taught us, that the potential for disrupting election processes in technology, by foreign or domestic actors is a serious and increasing concern. However, we as state election directors, we have had continued cooperation, and more effective communication, along with continued vigilance and innovation, will ensure the integrity of our voting processes and election results.

Again, we look forward to working with our federal partners as we plan for elections going forward. Thank you for the opportunity to share these thoughts and I'd be happy to answer any questions.

BURR: Thank you, Mr. Haas.

Mr. Sandvoss.

SANDVOSS: Good morning. Thank you, Chairman Burr, Vice Chairman Warner, and distinguished members of the committee. As Director of the State Board of Elections, I'd just like to briefly describe what our agency does. We are an independent bipartisan agency created by the 1970 Illinois constitution, charged with general supervision over the election, and registration laws in the state of Illinois.

As all of you seem to be aware, almost a year ago today, on June 23rd, the Illinois State Board of Elections was the victim of a malicious cyber attack of unknown origin, against the Illinois voter registration system database. Because of the initial low volume nature of the attack, the State Board of Election's staff did not become aware of it at first. Almost three weeks later, on July 12th, State Board of Elections IT staff was made aware of performance issues with the IVRS database server. The processor's usage had spiked to 100 percent with no explanation.

Analysis of the server logs revealed that the heavy load was a result of rapidly repeated data base queries on

the application status page of our paperless online voter application website. Additionally, the server log showed the data based queries were malicious in nature. It was a form of cyber attack known as SQL, which is structured query language injection. SQL injections are essentially unauthorized, malicious data base queries entered in to a data field, in a web based application.

We later determined that these SQLs originated from several foreign based IP addresses. SP programmers immediately introduced code changes to eliminate this particular vulnerability in our website. The following day, on July 13th, the SBE IT made the decision to take the website and IVRS database offline to investigate the severity of the attack. SBE staff maintained the ability to log and view all site access attempts.

Malicious traffic from the IP addresses continued, though it was blocked at the firewall level. Firewall monitoring indicated that the attackers were hitting SBE IP addresses five times per second, 24 hours a day. These attacks continued until August 12th, when they abruptly ceased. SV staff began working to determine the extent of the breech, analyzing the integrity of the IVRS database, and introducing security enhancements to the IVRS web servers and database.

A week later, on July 19th, we notified the Illinois general assembly of the security breech, in accordance with the Personal Information Protection Act. In addition, we notified the Attorney General's office. On July 21st, the State Board of Election's IT staff completed security enhancements and began to bring the IVRS system back online. A week after that, on July 28th, both the Illinois registration system, and the paperless online voting application became totally functional once again.

Since the attack occurred, the State Board of Elections has maintained the following ongoing activities the DHS scans the State Board of Election's systems for vulnerabilities, on a weekly basis. The Illinois Department of Innovation and Technology, which is a statewide entity that coordinates the IT systems of many of the Illinois state agencies, continuously monitors activity on the Illinois Century Network, which is the general network that provides firewall protection for the state computer systems.

This Department of Innovation and Technology, also called DOIT, provided cyber security awareness training for all state of Illinois employees, ours included. Now the State Board of Election's IT staff continues to monitor web server, and firewall logs on a daily basis. And in addition a virus protection software is downloaded, also on a daily basis. As a result of informing the Illinois Attorney General's office of the breach, the State Board of Elections was contacted by the Federal Bureau Investigation, and we have fully cooperated with the FBI in their ongoing investigation.

The FBI advised that we work with the Department of Homeland Securities, United States Computer Emergency Readiness team, to ensure that there is no ongoing malicious activity on any of the SBE systems. They also confirmed -- that is, the -- the Department of Homeland Security also confirmed that there's no ongoing malicious activity occurring in SBE computer systems.

To comply with the Personal Information Protection Act, nearly 76,000 registered voters were contacted as potential victims of the data breach. The SBE provided information to these individuals on steps to take if they felt that they were the victims of identity theft.

Additionally, the SBE developed an online tool to inform affected individuals of the specific information that was included in their voter record that may have been compromised.

As far as looking to -- for future concerns, one of the concerns facing our state and many others, we believe, is aging voting equipment. The Help America Vote Act established requirements for voting equipment, while -- but while initial funding was made available to replace the old punch-card equipment, additional funding has not been further appropriated.

If additional funding is not available, we would like to receive authorization to use the states' existing HAVA funds to allow spending on enhanced security across all election-related systems. The IVRS database is a federal mandate through the Help America Vote Act.

Cyber attacks targeting end users are also of particular concern. Security training funded and provided by a

federal entity such as the -- the EAC or DHS would also be beneficial, in our view.
In addition, any guidance or recommendations as to methods for the protection of registration and voting systems from cyber intrusions are always welcome.
Thank you for the time, and I'm happy to answer any questions.
BURR: Thank you, Mr. Sandvoss.
Dr. Halderman?
HALDERMAN: Chairman Burr, Vice Chairman Warner and members of the committee, thank you for inviting me to speak with you today about the security of U.S. elections.
I'm a professor of computer science, and have spent the last 10 years studying the electronic voting systems that our nation relies on. My conclusion from that work is that our highly computerized election infrastructure is vulnerable to sabotage, and even to cyber attacks that could change votes.
These realities risk making our election results more difficult for the American people to trust. I know America's voting machines are vulnerable, because my colleagues and I have hacked them, repeatedly, as part of a decade of research, studying the technology that operates elections and learning how to make it stronger.
We've created attacks that can spread from machine to machine, like a computer virus, and silently change election outcomes. We've studied touchscreen and optical scan systems, and in every single case, we found ways for attackers to sabotage machines and to steal votes. These capabilities are certainly within reach for America's enemies.
As you know, states choose their own voting technology, and while some states are doing well with security, others are alarmingly vulnerable. This puts the entire nation at risk.
In close elections, an attacker can probe the most important swing states or swing counties, find areas with the weakest protection and strike there. In a close election year, changing a few votes in key localities could be enough to tip national results.
The key lesson from 2016 is that these threats are real. We've heard that Russian efforts to target voter registration systems struck 21 states, and we've seen reports detailing efforts to spread an attack from an election technology vendor to local election offices.
Attacking vendors and municipalities could have put Russia in a position to sabotage equipment on Election Day, causing machines or poll books to fail, and causing long lines or disruption. They could have engineered this chaos to have a partisan effect, by striking places that lean heavily towards one candidate.
Some say the fact that voting machines aren't directly connected to the Internet makes them secure, but unfortunately, this is not true. Voting machines are not as distant from the Internet as they may seem.
Before every election, they need to be programmed with races and candidates. That programming is created on a desktop computer, then transferred to voting machines. If Russia infiltrated these election- management computers, it could have spread a vote-stealing attack to vast numbers of machines.
I don't know how far Russia got, or whether they managed to interfere with equipment on Election Day, but there's no doubt that Russia has the technical ability to commit widespread attacks against our voting system, as do other hostile nations. I agree with James Comey when he warned here, two weeks ago, we know they're coming after America, and they'll be back. We must start preparing now.
Fortunately, there's a broad consensus among cybersecurity experts about measures that would make America's election infrastructure much harder to attack. I've co-signed a letter that I ventured into the record from over 100 leading computer scientists, security experts and election officials that recommends three essential steps.
First, we need to upgrade obsolete and vulnerable voting machines, such as paperless touchscreens, and replace them with optical scanners that count paper ballots. This is a technology that 36 states already use. Paper provides a physical record of the vote that simply can't be hacked.
President Trump made this point well on Fox News the morning after -- the morning of the election. He said,

"there's something really nice about the old paper ballot system. You don't worry about hacking."
Second, we need to use the paper to make sure that the computer results are right. This is a common-sense quality control, and it should be routine.
Using what's known as a risk-limiting audit, officials can check a small, random sample of the ballots to quickly and affordably provide high assurance that the election outcome was correct. Only two states, Colorado and New Mexico, currently conduct audits that are robust enough to reliably detect cyber attacks.
Lastly, we need to harden our systems against sabotage and raise the bar for attacks of all sorts by conducting comprehensive threat assessments and applying cybersecurity best practices to the design of voting equipment and the management of elections. These are affordable fixes.
Replacing insecure paperless voting machines nationwide would cost $130 million to $400 million. Running risk-limiting audits nationally for federal elections would cost less than $20 million a year. These amounts are vanishingly small, compared to the national security improvement they buy.
State and local election officials have an extremely difficult job, even without having to worry about cyber attacks by hostile governments. But the federal government can make prudent investments to help them secure elections and uphold voters' confidence. We all want election results that we can trust.
If Congress works closely with the states, we can upgrade our election infrastructure in time for 2018 and 2020. But if we fail to act, I think it's only a matter of time until a major election is disrupted or stolen in a cyber attack.
Thank you for the opportunity to testify today, and for your leadership on this critical matter. I look forward to answering any questions.
BURR: Dr. Halderman, thank you.
The chair would recognize himself for five minutes. Members will be recognized by seniority.
Secretary Lawson, how many states is the secretary of state in charge of the elections process, do you know?
LAWSON: Yes, sir. It's 40. I'm sorry. Yes, sir. It's 40.
BURR: OK. Would you be specific, what do the secretary of states do -- what is it they do not like about elections being designated critical infrastructure?
LAWSON: The most important issue, sir, is that there have been no clear parameters set and even after the three calls that we had with Secretary Jeh Johnson, before the designation was made, we consistently asked for what would be different if the designation was made and how we would communicate. Would it be any different...
(CROSSTALK)
BURR: So nothing has negatively happened except that you don't have the guidance to know what to do?
LAWSON: Nothing has negatively happened to this date, but also, nothing positive has happened.
BURR: Got it. Got it.
Mr. Sandvoss, Illinois is one of the few states that have publicly been identified, I guess that's in part because you took the initiative to do it. You gave a good chronology, 23 June first sign, 12 July state I.T. staff took action, 12 August the attacks stopped.
At what point was the state of Illinois contacted by any federal entity about their system having been attacked or was it the state of Illinois that contacted the federal government?
SANDVOSS: We were contacted by the FBI -- I don't have the exact date but it was after we had referred the matter to the Attorney General's office. My guess would be probably a week after.
BURR: A week after...
(CROSSTALK)
SANDVOSS: After the A.G. was notified by us of this breach.
BURR: And the A.G. was notified approximately when?
SANDVOSS: On July 19th.
BURR: July 19th. OK. At what point did the state of Illinois know that it was the Russians?

SANDVOSS: Actually, to this day, we don't know with certainty that it was the Russians. We've never been told by any official entity. The only one, that we're aware of, that was investigating, was the FBI and they have not told us definitively that it was the Russians. Our I.T. staff was able to identify -- I think it was seven I.P. addresses from a foreign location, I believe it was the Netherlands.

But that doesn't mean that the attack originated in the Netherlands. We have no idea where it originated from.

BURR: Did your I.T. staff have some initial assessments on their own?

SANDVOSS: No, because I think any -- anything of that nature would have been speculative and we didn't want to do that. I think we wanted to leave that to the professional investigators.

BURR: You gave a update on what you're currently doing to enhance the security. DHS weekly security checks. Has the federal -- in your estimation, has the federal government responded appropriately, to date?

SANDVOSS: I believe they have, yes. I've heard nothing from our I.T. division and they'd be the persons that would know. I've heard nothing from them that the DHS's work in that matter has been less than satisfactory.

BURR: Let me ask all of you, except for you, Mr. Sandvoss. Do you believe the extent of cyber threats to election systems should be made public before the next election cycle?

Should we identify those states that were targeted, Mr. Haas?

HAAS: I think as election directors, we're certainly sensitive to the balance that Homeland Security and others need to make. I think so far -- as far as we've gone, we wanted to know, as the victims or potential victims. And then I think as part of the coordinating council and designation of critical infrastructure, there has to be a conversation amongst the election...

(CROSSTALK)

BURR: Is there a right of the public in your state to know?

HAAS: Yes, I believe there is. If there was a hack into our system, I think that our -- we would -- we would certainly want to consult our statutes and so forth, but we would -- we believe in transparency, we would want to let the public know.

BURR: Dr. Halderman?

HALDERMAN: I think the public needs details about these attacks, and about the vulnerabilities of the system, in order to make informed decisions about how we can make the system better and to provide the resources that election officials need. So, yes.

BURR: Secretary Lawson?

LAWSON: I lay awake at night worrying about public confidence in our election systems, and so, I think we need to be very careful and we need to balance the information because the worst thing that we can do is make people think that their vote doesn't count or it could be canceled out.

And so, if telling the public that -- you know, that these attacks are out there and our systems are vulnerable and it doesn't undermine confidence, it makes them know that we are doing everything we possibly can to stop those attacks, I'd be in favor of it.

BURR: I take for granted none of you at the table have evidence that vote tallies were altered in the 2016 election?

HALDERMAN: Correct.

BURR: Dr. Halderman, before I recognize the vice chairman real quickly, when you and your colleagues hacked election systems, did you get caught?

HALDERMAN: We hacked election systems as part of academic research, where we had machines in our facilities...

(CROSSTALK)

BURR: ...I get that. Did you get caught? Did they see your intrusion into their systems?

HALDERMAN: The one instance when I was invited to hack a real voting system, while people were watching, was in Washington D.C. in 2010 and in that instance, it took less than 48 hours for us to change all the votes

and we were not caught.
BURR: Vice chairman?
WARNER: I'd like to thank all the witnesses for their testimony. I find, a little stunning, Mr. Sandvoss, your answer. I don't know -- I think if you saw the preceding panel, you had the DHS and the FBI, unambiguously, say that it was the Russians who hacked into these 21 systems and I find it a little strange that they've not relayed that information to you.
What we discovered in the earlier testimony and that we finally got public disclosure that 21 states were attacked, and under question from -- from Secretary Harris, we found that even though we know those 21 states were attempted to be hacked into, or doors rattled, or whatever analogy you want to use, in many cases, the state election officials, whether the state directors or the secretaries of state, may not even have been notified. I find that stunning. And clearly, lots of local elected officials -- local election officials, where the activities really take place, haven't been notified. So I've got a series of questions and I'd ask for fairly brief responses. Dr. Halderman, can you just again restate, as Senator King mentioned in the earlier testimony, you don't need to disrupt a whole system, you could disrupt a single jurisdiction in a state, and you could, in fact, wipe that ledger clean, you could invalidate potentially not just that local election but then the results at the state -- the congressional level, the states, and ultimately, the nation, is that not correct?
HALDERMAN: Yes, that's correct.
WARNER: So we are not -- while it's important and I believe in our -- the centralized system, we are only as strong as our weakest link. Is that not correct?
HALDERMAN: That's correct.
WARNER: And Mr. Haas, and Secretary Lawson, do you believe that all 21 states that were attacked, that the state election officials are aware?
LAWSON: I can't answer that question, sir. I'm not certain. I will tell you that Indiana has not been notified. I don't know if we're even on the list.
HAAS: I don't know for sure, except that DHS did indicate in a teleconference that all the states that were attacked have been notified.
WARNER: We were told earlier that that's not the case. We were told that they may have been -- the vendors may have been notified. So do you know whether Wisconsin was attacked?
HAAS: We have not been told that -- that we were -- that there was an attack on Wisconsin.
WARNER: Are you comfortable, either one of you, with not having that knowledge?
LAWSON: We are hypersensitive about our security and I would say that when the FBI sent the notice in September, for states to look for certain I.P. addresses to see if their -- their systems had been penetrated, or attempted to be penetrated, we absolutely searched -- in fact, we looked at 15,500,000 log-ins that had happened in our system since the first of January that year.
And so we -- we believe that our system has not been hacked.
HAAS: I would also state that both our office and the chief information officer of the state, and his office, would likely be able to detect that the system was hacked...
(CROSSTALK)
WARNER: Well just, we've got the two leading state election officials not knowing whether their states were one of the 21 that, at least, the Russians probed -- let me finish, please. And you know, I see -- I understand the balance. But the notion that state election officials wouldn't know -- wouldn't know, that local election officials clearly haven't been notified, I appreciate the chairman's offer.
The chairman and I are going to write a letter to all the states. If you view yourself as victims, I think there is a public obligation to disclose. Again, not to re-litigate 2016, but to make sure that we're prepared for 2017, where I have state elections in my state this year, and 2018. And it's -- to do otherwise because there are some -- there are some still in the political process that believe this whole Russian incursion into our elections is a witch

hunt and fake news.
So I could very easily see some local elected officials saying "this is not a problem, this is not a bother. I don't need to tighten up my security procedures at all." And that would do a huge, huge disservice to the very trust, Secretary Lawson, that you say you want to try to present and provide for our voters. So I hope when -- when you receive the letter from our -- and we're going to write this on a confidential basis, but that you would urge your colleagues to come forward, again, not to embarrass any state.
But I find it totally unacceptable, one, that the public doesn't know, that local elected officials -- local election officials don't know that you as two -- as the leaders of the state election officials don't even know whether your states were part of the 21 that has been testified by the DHS that, at least, they were, if not looked at, door jiggled, or actually is the case in Illinois, where actual information from the voter registration efforts were exfiltrated.
So my hope is that you will work with us on a cooperative basis and we want to make sure that the DHS and others are better at sharing at information and you get those classified briefings that you deserve.
BURR: Senator Risch.
RISCH: Thank you very much.
Mr. Sandvoss, I -- July 12th was the date that you first discovered that you had issues. Is that right?
SANDVOSS: Yes, that's correct.
RISCH: And that was a result of a high-volume spike. Is that correct?
SANDVOSS: Yes, that is correct.
RISCH: Then when you looked at it, you found out that the intrusion attempts actually had started June 23rd, is that correct?
SANDVOSS: Yes.
RISCH: So -- and those were low-volume spikes, starting on June 23rd.
SANDVOSS: Yes.
RISCH: All right. So, if they had never cranked up the volume, is it fair to say you would have never discovered it? Or probably wouldn't have discovered it?
SANDVOSS: I would say it would probably not have been discovered -- certainly not right away. And if it was -- the volume was low enough, even an analysis of our server logs might not catch something like that, because it wouldn't stand out.
So I think the answer to your question is yes.
RISCH: Then you said 12 -- or seven days later, the 19th, you notified the attorney general. Is that right?
SANDVOSS: Yes, correct.
RISCH: That was the -- that was the Illinois attorney general, not the U.S. attorney general, is that correct?
SANDVOSS: Yes. State law requires that we notify the attorney general in these instances.
RISCH: So then the next thing that happened is you were contacted by the FBI. Is that correct?
SANDVOSS: Yes.
RISCH: All right. So the question I've got, I'm just -- I'm just trying to get an understanding the facts -- are you assuming that the Illinois A.G. contacted the FBI, or do you know that, or not know that, or (OFF-MIKE).
SANDVOSS: I don't know that for sure, but I -- I would suspect that they probably did, because how else would the FBI know?
RISCH: Right. Well, and that's kind of where I was getting, is that -- that was not the result of some federal analysis -- that there wasn't a federal analysis of this that turned up what had actually happened. Is that -- is that a fair statement?
SANDVOSS: I believe so, yes.
RISCH: You then did some things to try to mitigate what had happened. Had you -- had you shared this with other states, as to what you had done, in order to, I don't know, develop a best practices, if you would?

SANDVOSS: We didn't have any formal notification to all 50 states, no. I think our focus at that time was trying to repair the damage and assess, you know, what needed to be done, especially with respect to the voters who had their, you know, information accessed.

I believe that, once the FBI got -- became aware of this, I know they contacted the different states. I don't believe our attorney general's office did, although I don't know that for certain. But we did not have any formal communication with all 50 states regarding this.

RISCH: And do you believe that you have developed a best- practices action after this attack that you described for us?

SANDVOSS: I believe so, yes.

RISCH: You think it would be appropriate for you to get that out through the secretary of states organization, or other organizations, so that other states could have that.

SANDVOSS: Certainly. Absolutely.

RISCH: OK.

Mr. Halderman, Your hacking that you've described for us -- does -- would your ability -- if you were sitting in Russia right now, wanted to do the same thing that you had done, would that ability be dependent upon the machines, or whatever system is used, being connected to the Internet?

HALDERMAN: That ability would depend on whether pieces of election I.T. equipment -- I.T. offices that are where the election programming is prepared are ever connected to Internet. The machines themselves themselves don't have to be directly connected to the Internet for -- for a remote attacker to target them.

RISCH: So would recommend that -- that the voting system be disconnected from the Internet, that it be a standalone system that can't be accessed from the outside?

HALDERMAN: It's a best practice, certainly, to isolate vote tabulation equipment as much as possible from the Internet, including isolating its -- the systems that are used to program it.

But other peoples of election infrastructure that are critical, such as electronic poll books or online registration systems, do sometimes need to be connected to Internet -- to systems that have Internet access.

RISCH: But that wouldn't necessarily require that it be connected to the Internet for the actual voting process. Is that right?

HALDERMAN: That's right.

RISCH: And then the extrication of that information off of the voting machine -- would that be fair?

HALDERMAN: The -- I think that's fair to say.

RISCH: Thank you.

Mr. Chairman, I think all of this really needs to be drilled down a little bit further, because it seems to me, with this experience, there's probably some really good information where you could put a firewall in place that -- to stop that -- at least minimize it.

Thank you.

BURR: Senator Wyden.

WYDEN: Thank you, Mr. Chairman. And thank -- thank all of you.

I want to start with you, Professor Halderman. What are the dangers of manipulation of voter registration databases, particularly if it isn't apparent until Election Day, when people show up at the polls to vote?

HALDERMAN: I'm concerned that manipulating voter registration databases could be used to try to sabotage the election process on Election Day.

If voters are removed from the registration database, and then they show up on Election Day, that's going to cause -- cause problems. If voters are added to the voter registration database, that could be used to conduct further attacks.

WYDEN: Let me ask, and this can be directed at any of you. I'm trying to get my arms around this role of contractors and subcontractors and vendors who are involved in elections. Any idea, even a ball park number,

of how many of these people there are? Ten, 70, 200?
HALDERMAN: Vendors that host the voter registration system -- I'm sorry, Senator, I don't have a number.
LAWSON: Sir, I don't have an exact number either, but I will -- I will tell you, in Indiana, for an example, we have six different voting system types. Counties make that decision on their own. But they are all certified by our voting system technical oversight program.
WYDEN: That was my main (ph) question.
So somebody is doing certification over these contractors and subcontractors and equipment vendors and the like? Does that include voting machines, by the way? LAWSON: It does. Most states will have a mechanism to certify the voting machines that they're using, the electronic poll books they're using, the tabulation machines that they're using, making sure that they comply with federal and state law, and making sure that they have the audit processes in place.
WYDEN: So you all have a high degree of confidence that these certification processes are not leaving this other world of subcontractors and the like vulnerable?
HALDERMAN: I have several concerns about the certification processes, including that some states do not require certification to federal standards; that the federal standards that we have are unfortunately long overdue for an update and have significant gaps when it comes to security. And that the certification process doesn't necessarily cover all of the actors that are involved in that process, including the day-to-day operations of companies that do pre-election programming.
WYDEN: One last question. We Oregonians and a number of my colleagues are supportive of our efforts to take vote-by-mail national. And we've had it. I was in effect the country's first senator elected by vote-by-mail in 1996. We've got a paper trail. We've got air gap computers. We've got plenty of time to correct voter registration problems if there are any.
Aren't those the key elements of trying to get on top of this? Because it seems to me, particularly the paper trail. If you want to send a message to the people who are putting at risk the integrity of our electoral institutions, having a paper trail is just fundamental to being able to have the backup we need.
I think you're nodding affirmatively, Professor Halderman, so I'm kind of inclined -- or one of you two at the end were nodding affirmatively, and I'll quit while I'm ahead if that was the case -- but would either of you like to take that on?
HALDERMAN: Vote-by-mail has significant cybersecurity benefits. It's very difficult to hack a vote-by-mail system from an office in Moscow. There are -- whether vote-by-mail is appropriate for every state, in every context, is in our system of course a matter for the states, but I think it offers positive security benefits.
WYDEN: All right.
Thank you, Mr. Chairman.
BURR: Senator Blunt?
BLUNT: Dr. Halderman, on that last answer to that last question, how do you count vote-by-mail ballots?
HALDERMAN: Generally, they would be counted using optical scanners.
BLUNT: Exactly. So you count them the same way you count ballots that aren't vote-by-mail in almost every jurisdiction?
HALDERMAN: If the optical scan ballots are subsequently audited, you can get high security from that process, but yes.
BLUNT: Well that's a different -- that's a different question. Your question there is do you prefer paper ballots and an audit trail, and I do too, but let's not assume that the vote-by-mail ballots are counted any differently. They're counted probably at a more central location, but that doesn't mean that all the manipulation you talked about that we need to protect against wouldn't happen in a vote-by- mail election. You've got a way to go back and you've got a paper trail to count.
HALDERMAN: That's correct. There are three things you need: paper, auditing, and otherwise good security

practices.
BLUNT: While I've got you there, on auditing, how would you audit a non-paper system? If it's a touch-screen system, you mentioned Colorado, and New Mexico already did a required sample audit, which I'm certainly not opposed to that if that's what states want to do, or is the best thing to do. How would you do a non-paper audit?
HALDERMAN: Senator, I think it would be difficult or impossible to audit non-paper systems with the technology that we use in the United States, to a high level of assurance.
BLUNT: So even if you -- if you don't have something to audit, it's pretty hard to audit a system that counted -- that didn't leave a trail.
HALDERMAN: It's basically impossible.
BLUNT: So, Mr. Sandvoss, in Illinois, do you certify counting systems?
SANDVOSS: Yes, we do.
BLUNT: And Secretary Lawson, do you certify counting systems?
LAWSON: Yes, sir.
BLUNT: Mr. Haas, in your, your jurisdiction, somebody is certifying those systems that you use?
HAAS: We both rely on the EAC certification and then our commission does a testing protocol and then approves the equipment to be used in the state of Wisconsin.
BLUNT: And back in Illinois, do you then monitor, in any way, that counting system while it's doing the actual counting?
SANDVOSS: No, the actual counting done on Election Day, Election Night, rather, is done locally at the County Clerk's offices or Board of Election Commissioner offices. We certify the voting equipment -- they have to apply for certification and approval, which we conduct a fairly rigorous test of the voting equipment, but then in actual practice, other than -- we do conduct pre-election tests of the voting equipment on a random basis before each election, but there -- it's a limited number of jurisdictions.
BLUNT: And do you do that in a way that allows you, from your central office, to get into the local system? Or do you go to the local jurisdictions or just monitor how they count that -- how they, how they check that counting system?
SANDVOSS: When we do our pre-election tests, we actually visit the jurisdiction.
BLUNT: All right.
Secretary Lawson, similar?
LAWSON: Similar, however, the State does not go into the Counties, but the Counties are required to do a public test, and as I mentioned, it's public. And so they're required to do testing on the machines, the tabulation, there's a bipartisan election board that's there...
(CROSSTALK)
BLUNT: I guess the -- I guess the point I'd want to drive home there is, that not opening that door to the counting system -- if you don't have the door, nobody else can get through that door as well. But there's monitoring, there's local testing, I don't suggest at all that Dr. Halderman's comments aren't important or something we should guard against, it's -- I was an election official for twenty years, including the Chief Election Official for eight of those, and something -- as we were transitioning to these systems -- something I was always concerned about is what could possibly be done that could be done and undetected.
One of the reasons I always liked the audit trail -- that obviously, Dr. Halderman, you do, you do too, is that you do have something to go back -- if you have a reason to go back -- and really determine what happened on Election Day. Let's talk for just a moment about the much more open registration system.
Secretary Lawson, you said you had 15,500 logins. I believe that was -- talk about logging -- what are they logging into, there? The statewide voter registration system that you maintain a copy of?
LAWSON: The 92 County Clerks in Indiana are connected to the statewide voter registration system, and that 15,500,000 logins reflected the work that they did that year.

18-F-1517//1079 ProQuest

BLUNT: 15,500,000?
LAWSON: 15,500,000.
BLUNT: So, obviously, that's a system that has lots of people coming in -- in and out of that system all the time. Do local jurisdictions, like if the library does registration, do you have counties where they can also put those registrations directly into the system?
LAWSON: Other than the counties, no sir. But we do have Indianavoters.com, where a voter can go on and register themselves. And it's a record that is compared to the BMV record, and then the counties will find that information in their hopper the next day. And then they will -- or their computer system, and then the next day they will have the ability to determine whether or not the application is correct.
BLUNT: Do all of your jurisdictions, the three jurisdictions here reflected, have some kind of provisional voting, if you get to the voting place on Election Day and your address is wrong, or your name is wrong, or it doesn't occur -- it doesn't appear at all? Do you have a way somebody can cast a ballot before they leave?
LAWSON: Yes, sir.
BLUNT: And in Illinois?
SANDVOSS: Yes, we do.
HAAS: We have provisional ballots, but they are very limited. We are not an NVR -- NVRA state. And we also have Election Day registration, so people can register at the polls.
BLUNT: So, the failure to have your name properly on the -- I understand, Chairman, and I also noticed the time on others. But just -- the registration system is much more open than the tallying system, that doesn't mean the tallying system doesn't need to be further protected. But the registration system, the idea that somebody gets into the registration system -- there are plenty of ways to do that. Unfortunately, we think now other countries and governments may be doing that as well.
BURR: Senator King?
KING: Thank you, Mr. Chairman.
Dr. Halderman, you're pretty good at hacking voting machines, by your testimony. Do you think the Russians are as good as you?
HALDERMAN: The Russians have the resources of a nation-state. I would say their capabilities would significantly exceed mine.
KING: I expected that was going to be your answer, but I wasn't sure whether your modesty would -- but I think that's an important point, because you testified here today that you were able to hack into a voting machine in 48 hours, change the results, and nobody knew you had done it.
And if you could do it, I think the point is, the Russians could do it if they chose. And we've been talking a lot about registrations lists. My understanding is that, quite often, a voter registration list, at some point in the process, is linked up with -- the computer that has the voter registration list, is linked up with configuring the voting machines, and perhaps even tallying votes. Is that true? Can any of you...
(CROSSTALK)
LAWSON: No, sir.
KING: There's -- there's no connection between the registration list and the voting machines?
LAWSON: No.
KING: Illinois? Is that...
(CROSSTALK)
SANDVOSS: Not in Illinois, no.
KING: OK.
HAAS: That's correct. KING: Well, then I was mistaken. Hm?
Yes, Dr. Halderman?
HALDERMAN: I believe that depends on the specific equipment involved. There may be some designs of voting

systems where there -- the sign-in and the vote counting system are linked.
KING: But of course, if, as you testified I think, if the voting registration list is tampered with in some way, on Election Day, it would be chaos. If names disappeared, people arrived at the polls and their names weren't on the list. Isn't that correct, Ms. Lawson?
LAWSON: If a person showed up at the polls to vote and their name wasn't on the list, if they were expecting they would be given a provisional ballot, I think the biggest danger is that the lines at the polls would increase significantly, if there was a large number of folks who had to do that in each precinct.
KING: Right, that was what I was referring to. On August 1st of 2016, press reports have indicated that there was an FBI notification to all of their field offices about the danger of cyber intrusions into voting systems. Supposedly, those were passed on to state election systems. Did you three get something from the FBI around August 1st that gave IP addresses and some warnings about what should be done?
SANDVOSS: Yes, we did receive an FBI flash. It was in August, and you're saying the 1st, I believe that was it.
KING: That was, yeah, I understand that was the date of it.
Ms. Lawson, did you receive that?
LAWSON: Yes, Indiana received a notice from the FBI.
HAAS: We did, as well.
KING: So there is some interconnection. I mean, one of the things that I'm sort of hearing, and I'm frankly appreciative and happy that you all did receive that notice, but there seems to be a lack of information sharing that goes on that we really need to be sure that -- for example, if you learn -- if something happens in Illinois -- some system whereby you can alert your colleagues across the country to look out for this. And if we learn things here in Washington, if the FBI learns things, that they can alert people around the country, because the best time to deal with this is before the election. After the election, or on Election Day, is much more difficult.
Dr. Halderman?
HALDERMAN: Yes, I would support further information sharing.
KING: And then finally, we've talked about what we do about this. Paper trails has come up. Is that the principal defense? Is that -- Dr. Halderman, what if -- I asked the question to the prior panel. What would you tell my elections clerk in Brunswick, Maine, would be the three things most important that they should do, or my secretary of state in Maine, to protect themselves against a threat we know is coming?
HALDERMAN: The most important things are to make sure we have votes recorded on paper, paper ballots, which just cannot be changed in a cyber attack, that we look at enough of that paper in a post- election, risk limiting audit, to know that they haven't -- the electronic records haven't been changed.
And then, to make sure we are generally increasing the level of our cyber security practice. Information sharing is an example of a good and recommended practice, as are firewalling systems and other things that have been suggested.
KING: One final question. Is it possible -- and we -- there are some press reports about this, of a cyber attack on the vendors of these machines, to somehow tamper with the machines before they go out to the states. Is that a risk?
HALDERMAN: I would be concerned about that. And, in fact, the small number of vendors is an example of how our system in practice is not quite as decentralized as it may appear -- that attacks spreading via vendors, or from vendors to their customers, could be a way to reach voting equipment over a very large area.
KING: And there have been press reports that that -- that, in fact, was attempted in 2016.
HALDERMAN: Yes, that's correct.
KING: Thank you, Mr. Chairman. Mr. Chairman, I want to thank you for holding this hearing. This is such important information for the public, and for our democracy. I appreciate your work here.
BURR: Thank you, Senator.
Senator Harris?

HARRIS: Thank you. So there's a saying that I'm sure many of you have heard, which is the -- you know the difference between being hacked and not being hacked, is knowing you've been hacked. And so I appreciate, Dr. Halderman, the recommendations that you and your colleagues have made, because it also seems to cover the various elements of what we need to do to protect ourselves as a country in terms of our elections, which is prevention, and then there's the issue of detection and also resilience.

Once we -- if we discover that we've been manipulated, let's have the ability to stand back up as quickly as possible. So I have a few questions in that regard. First of all, have each of you -- you received the -- for the states -- received a notification from the FBI? Is that correct?

LAWSON: Yes, ma'am. HAAS: Yes, yes.

SANDVOSS: Yes.

HARRIS: And were any of you also notified by DHS?

Mr. Sandvoss?

SANDVOSS: We had communications with DHS, I don't recall how they were initiated. But I do know that there have been some -- the conference calls with them, and it may have been through the FBI that that occurred.

HARRIS: And I'm speaking of before the 2016 election.

SANDVOSS: Yes.

HARRIS: Yeah.

SANDVOSS: Yes.

HARRIS: Secretary Lawson?

LAWSON: Yes, we had -- we did have conversations with Department of Homeland Security. However, it was through our national association, it was not a direct contact with the state.

HARRIS: Thank you.

HAAS: We were one of the states that took up DHS on their offers to do the cyber hijinks scan. We did have a number of communications with, I believe, a point person in their Chicago office. The FBI alert I think was about a specific incident, but our communications with DHS were more about general steps that could be taken to protect our systems.

HARRIS: So, as a follow-up to this hearing, if each of you -- to the extent that you can recall the nature of those conversations with DHS before the election, if you could share that with the committee, that would be helpful, so we can figure out how notifications might be more helpful to you in the future. If -- hopefully they're not necessary, but if necessary.

Can you, Ms. Lawson, tell me -- Secretary Lawson -- what, in your opinion, are the pros and cons of requiring states to report to the federal government if there's been a breach or a hack? What can you imagine would be the pros and cons of a policy that would require that?

LAWSON: Well, the pro would be that if there -- if, for an example, the FBI or the Department of Homeland Security has better ways to counter those attacks, or to make sure that the reconnaissance is done after such an attack is more sophisticated than the states, then obviously, that would be a pro. Indiana did not take the opportunity to have DHS do our cyber cleaning because we felt that we were in better shape than what they could provide for us, so that would be the con.

HARRIS: OK. And can you, Professor Halderman, tell me -- you know we -- before this last election cycle, there had been a lot of talk through the years, in various states -- Senator Blunt, I'm sure you were part of those discussions about the efficacy of online voting, because it would bring convenience, speed, efficiency, accuracy -- and now we can see that there will be great, potentially, vulnerabilities by doing that. So can you talk with me a little about -- just in terms of policy -- is the day of discussing the need for online voting, has that day passed because of the vulnerabilities that are associated with that?

HALDERMAN: I think that online voting, unfortunately, would be painting a bullseye on our election system. Today's technology just does not provide the level of security assurance for an online election that you would

need in order for voters to have high confidence.

And I say that, having myself done -- hacked an online voting system that was about to be used in real elections, having found vulnerabilities in online voting systems that are used in other countries. The technology just isn't ready for use.

HARRIS: And isn't that the irony, that the professor of computer engineering -- and I would -- always believed that we need to do more to adopt technology, that government needs to adopt technology -- I think we're advocating good old days of paper voting are the way to go, or at least an emphasis on that, instead of using technology to vote.

Can you tell me also -- any of you, if you know -- it's my understanding that some of the election system vendors have required states to sign agreements that prevent or inhibit independent security testing. Are you familiar with that?

HALDERMAN: That certainly had been something that inhibited attempts by researchers like me to study election systems in the past.

HARRIS: And do you believe that that's a practice that is continuing?

HALDERMAN: I do not -- I don't know the answer to that question.

HARRIS: Have any of you had that experience with any of your vendors?

SANDVOSS: In Illinois, no, we have not. And I don't think Illinois law would allow such an agreement.

LAWSON: I don't believe that would happen in Indiana either, Senator, because in order to sell voting equipment in the state of Indiana, it has to be certified.

HARRIS: Right, which would require testing.

LAWSON: Yes, which requires testing. HARRIS: Thank you, thank you, Mr. Chairman. Thank you.

BURR: Thank you, Senator Harris.

Any Senators seek additional questions or time? Seeing none, let me wrap up. I want to thank all of you for your testimony today.

Secretary Lawson, to you. I really encourage you, as the next representative of secretaries of states, to remain engaged with the federal government, specifically the Department of Homeland Security. And I think with any transition of an administration, there is a handoff and a ramp-up. And I've been extremely impressed with our witness from DHS, who not only was here today, but she has taken the bull by the horns on this issue, and I think you'll see those guidelines very quickly, and I hope that there will be some interaction between secretary of states, since in 40 states you control the voting process.

And you can find the system of federal guidance and collaboration that works comfortably with every secretary of state in your organization. I think it is absolutely critical that we have not only a collaboration, but a communication between the federal government and the states as it relates to our voting systems. If not, I fear that there would be an attempt to, in some way, shape or form, nationalize that.

That is not the answer, and I'll continue to point, Mr. Sandvoss, to Illinois. It is a great example of a state that apparently focused on the IT infrastructure, in staff, and didn't wait for the federal government to knock on the door and say, hey, you got a problem. You identified your problem, you began to remediate it. At some point, the federal government came in as a partner, and I think where we see our greatest strength is to work with states and to chase people like you, Dr. Halderman, who like to break into -- no, I'm just kidding with you. Listen, I think what you did is important.

And I think the questions that you raised about the fact that you really can target to make the impact of what you're trying to do very, very effective. And that's clearly what campaigns do every day. So we shouldn't be surprised if the Russians actually looked at that, or anybody else who wants to intrude into our voting system and our democracy in this country. The -- I've got to admit that the variation of voting methods, six in Indiana, where I don't know how many counties you've got -- I've got 100 counties in North Carolina -- it may be that I find out that every county in North Carolina has the power to determine what voting machines, what voting

software they have.

This can get extremely complicated. Short of trying to standardize everything, which I don't think is the answer, is, how do we create the mechanism for the federal government to collaborate directly with those heads of election systems in the states, and understand up front what we bring to the table, and how we bring it so that we're all looking at the same thing -- the integrity of every vote going to exactly who it was intended to do. So we're going to have debates on paper or electronic, we're going to have debates on what should the federal role be -- at the end of the day, if we haven't got cooperation, and collaboration and communication, I will assure you we will be here with another Congress, with another makeup of the committee, asking the same questions, because we won't have fixed it.

But I think that what Dr. Halderman has said to us is, there are some ways that we can collectively approach this, to where our certainty of intrusions in the future can go down. And the accuracy of the vote totals can be certified. So I thank all the four of you for being here today in our second panel. This hearing is now adjourned.

END

Subject: State elections; Voting machines; Collaboration; National security;

Location: United States--US

Company / organization: Name: National Association of Secretaries of State; NAICS: 813910;

Publication title: Political Transcript Wire; Lanham

Publication year: 2017

Publication date: Jun 21, 2017

Publisher: CQ Roll Call

Place of publication: Lanham

Country of publication: United States

Publication subject: Political Science

Source type: Wire Feeds

Language of publication: English

Document type: News

ProQuest document ID: 1912764930

Document URL: https://search.proquest.com/docview/1912764930?accountid=14026

Copyright: 2017 Bloomberg Government

Last updated: 2017-06-23

Database: Global Newsstream,ABI/INFORM Trade & Industry

Contact ProQuest

Copyright © 2017 ProQuest LLC. All rights reserved. - Terms and Conditions

18-F-1517//1080

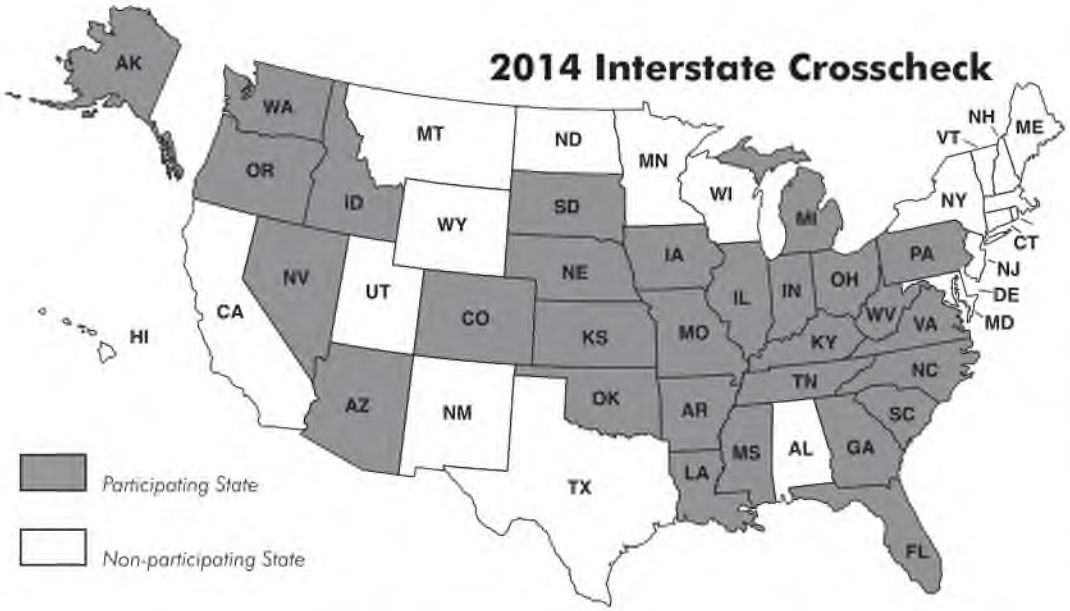
Exhibit 33

canvassing kansas
AN UPDATE ON ELECTION NEWS FROM THE KANSAS SECRETARY OF STATE'S OFFICE

DECEMBER
2013

Interstate Crosscheck Program Grows

The ninth annual data comparison for the interstate voter registration crosscheck program will be run in January 2014. The program has grown from its original four midwest states (Iowa, Kansas, Missouri and Nebraska) to 29 states in 2014. In 2012 there were 15 participating states and in 2013 there were 22.



The interstate crosscheck program, administered by the Kansas Secretary of State's office, began in December 2005 when the secretaries representing the four original states signed a Memorandum of Understanding to coordinate their offices' efforts in several areas of election administration. Crosschecking voter registration data was one of the areas cited. The first crosscheck was conducted the next year, in 2006.

The program serves two purposes: (1) it identifies possible duplicate registrations among states, and (2) it provides evidence of possible double votes. Most states, including Kansas, process the duplicate registrations by mailing the individuals confirmation notices (as provided in the National Voter Registration Act of 1993) and placing the individuals' names in inactive status. Inactive voters are those for whom election officers have received evidence that they have moved out of the county or state. Once they are given inactive status, their registrations may be canceled if they fail to vote or otherwise contact the election office from the date of the confirmation notice through the second succeeding federal general (November) election.

Cont'd on pg. 6

IN THIS ISSUE

18-F-1517//1082

canvassing kansas

Published by the Office of the Secretary of State

EDITORS
Brad Bryant
Kay Curtis

LAYOUT AND DESIGN
Todd Caywood

CONTRIBUTORS
Brad Bryant
Kay Curtis

Suggestions or comments? Please call (785) 368-8095.

This publication may be duplicated for informational purposes only. No written permission is required with the exception of articles or information attributed to a source other than the Kansas Secretary of State.

© 2013

Kansas Secretary of State
Memorial Hall
120 SW 10th Ave.
Topeka, KS 66612-1594
(785) 296-4564

From the desk of the Secretary

"Lead, follow, or get out of the way."
Thomas Paine, 1737 - 1809. Kansas has consistently chosen the former when it comes to elections.

In 2005 Kansas took the lead when four states agreed to compare voter registration records with each other annually in order to identify duplicate voter registrations and double votes. Our IT department pulls data from a secure FTP site, runs comparisons and uploads the results to the FTP site on January 15 each year. Then each participating state can download its results and process them according to their own laws and regulations. The Interstate Voter Registration Crosscheck Program had increased to 14 participating states when I took office in 2011.

Convinced of the value of the program, I decided that I would make it one of my highest priorities to increase the number of participating states, hopefully doubling its size. The more states that participate, the more duplicate records each participating state can find. I contacted chief election officers in other states to explain how Crosscheck works and the value of this tool to maintain clean, current, and accurate voter lists to fight voter fraud. As a result, the number of states participating has more than doubled to 29 states that will share voter registration data in January 2014. While I am very pleased that over half of the 50 states are currently on board, I will continue to promote Crosscheck as an effective means of list maintenance.

In 2008 Kansas took the lead in helping voters to find election information when they need it by using internet search engines. As part of the Voting Information Project (VIP), Kansas contracted with ES&S to make programming changes to our ELVIS database so that all states with ES&S can provide a data feed to the VIP program which hosts the data. Google acknowledged our contribution by presenting a Kansas-shaped VIP award to the State of Kansas at the summer NASS conference.

Finally, in 2011 Kansas took the lead as the first state to combine three election-security policies: (1) requiring a government-issued photo ID for voting in person, (2) requiring either a Kansas driver's license number or photocopy of a current photo ID for applying for a mail-in ballot, and (3) requiring a document proving U.S. citizenship when a person registers to vote for the first time. Consequently, Kansas elections are the most secure in the nation against fraud.

Thank you for all you have done to help implement these reforms. Together we have made Kansas the nation's leader.

Kris W. Kobach

18-F-1517//1083

Voting Information Project Award Received at NASS

On July 19th, 2013, Google presented an award to recognize Kansas' efforts to improve the efficiency and effectiveness of elections through open data. Eight other states also received the award at the National Association of Secretaries of State 2013 Summer Conference in Anchorage, Alaska. Each of the nine states had participated in the Voting Information Project (VIP) by publishing polling places and other election data as part of the open data effort. Secretary of State Kris Kobach was present to accept the award for his office.

By joining the project on the ground floor, Kansas was among the first states to help registered voters to more readily find election information when they need it and where they are most likely to look for it. Government websites often are not the first place voters look. VIP is similar to the online VoterView feature of the Kansas voter registration system, and voters who perform Google searches for voter registration information will end up at the VoterView website as a result of the VIP.

In the run up to the 2012 general election, 22 million times users queried the Google Civic Information API. According to the VIP program, "When the project started in 2008, nobody involved knew whether the open data effort would have any impact at all. Early adopters took a risk on something new by agreeing to participate and the payoff was immense."

Google award presented to the state of Kansas for its contribution to the Voting Information Project.
Photo by Todd Caywood

The VIP program was initiated as a cooperative effort between the Pew Foundation and Google. As a private charitable organization, Pew's rules do not allow them to pay money to a private for-profit corporation, so Pew asked the Kansas SOS office to serve as a go-between. The SOS office wrote specifications and requested Election Systems & Software to make the required programming changes in the voter registration database. The cost of the programming was paid by Pew to the SOS office and passed on to ES&S. As a result, all states with ES&S databases benefit from the new functionality.

For more information about Kansas participation in the VIP project since 2008, see Canvassing Kansas, September 2010, page 6. ■

Clemens Receives CERA Certification

Crystal Clemens, Seward County Deputy Clerk/Election Officer, completed the Election Center's CERA program this year. Certificates were presented at the Election Center's annual national conference in Savannah, GA, held August 13-17, 2013. Crystal was one of fifty eight election officials to receive the award this year.

CERA (Certified Elections/Registration Administrator) is one of very few nationally recognized programs providing professional training for election administrators. The Election Center itself is a nationwide professional association of local, county and state voter registrars and election administrators that promotes training and best practices, monitors and lobbies on federal legislation, and provides a forum for the exchange of ideas.

Completion of the CERA program requires travel and attendance at a number of training sessions across the country over a period of years. Crystal is one of a small handful of Kansas election officials who have completed it.

Crystal's supervisor, Seward County Clerk Stacia Long, had this to say: "Crystal has always shown great passion for the entire election process. I am very proud of her designation as a CERA. She truly is a great asset to the Election Office and Seward County." ■

Attorney General Issues Opinion on Concealed Carry

The office of Attorney General Derek Schmidt issued a formal opinion on November 27, 2013 in response to questions posed by Secretary of State Kris Kobach. Kobach requested the opinion in a letter dated September 30, 2013, as chief state election officer and on behalf of county election officers across the state.

The issue at the heart of the request was how polling places would be affected by passage of the Personal and Family Protection Act of 2013. The Act, passed as Senate Substitute for House Bill 2052 (2013 Kansas Session Laws, Chapter 105), authorizes persons who possess concealed carry permits to carry weapons into municipal buildings except under specific circumstances. "Municipal building" includes any facility owned or leased by a municipality, which could include facilities used as polling places during advance voting or on election day.

In his letter, Secretary Kobach asked the following questions:

1. ***Does the Act apply to privately-owned facilities used as polling places by verbal agreement?***

2. ***Does the Act apply to privately-owned facilities used as polling places by written agreement when no rent money is paid to the owner or manager of the site?***

3. ***Does the Act apply to privately-owned facilities used as polling places by written agreement when rent money is paid to the owner or manager of the site?***

4. ***If only one room or one portion of a building otherwise not subject to the Act is used as a polling place, does the Act apply to the entire building or only to the area used as a polling place?***

5. ***If an area in a nursing home, assisted living center or long term care facility is used for mobile advance voting pursuant to K.S.A. 25-2812, does the Act apply to the voting area?***

6. ***Do the provisions of the Act applicable to schools still apply to school facilities used as polling places?***

7. ***Is a county government liable for claims of denial of equal protection if various polling places have different levels of security as a result of implementation of the Act?***

At the time of this writing, the secretary of state had just begun to analyze the opinion. The SOS office will communicate further information to CEOs when the analysis is complete. In the meantime, CEOs are encouraged to discuss the opinion with their county attorneys and counselors. The full opinion may be found online: ***http://ksag.washburnlaw.edu/opinions/2013/2013-020.pdf***.

The synopsis from Attorney General Opinion 2013-20 is reproduced here:

Except as described herein, the use of real property as a polling place does not transform the nature of that property for the purposes of the PFPA. Any concealed carry requirements that applied to that property immediately before its temporary use as a polling place continue to apply during its use as a polling place and thereafter.

The Personal and Family Protection Act (PFPA) authorizes concealed carry licensees to carry a concealed handgun into a polling place to the extent that concealed handguns are permitted to be carried into the building in which the polling place is located.

The provisions of K.S.A. 2013 Supp. 75-7c20 apply only to buildings that are owned or leased in their entirety by the state or a municipality. If the PFPA requires concealed carry to be permitted in a state or municipal building, then concealed carry licensees must be permitted to carry a concealed handgun in all parts of the building, including areas used as polling places, with the exception of courtrooms, ancillary courtrooms, and secure areas of correctional facilities, jails and law enforcement agencies.

The governing body or chief administrative officer, if no governing body exists, of a state or municipal building may exempt the building from the provisions of K.S.A. 2013 Supp. 75-7c20 for a set period of time. If a state or municipal building is so exempted, concealed carry may be prohibited by posting the building in accordance with K.S.A. 2013 Supp. 75-7c10.

Cont'd on pg. 6

18-F-1517//1085

SOS Office Involved in Litigation

The office of the Kansas Secretary of State finds itself involved in three lawsuits that could affect the voter registration process and the 2014 elections. All are related to the 2011 Kansas SAFE Act. One case deals with the photo ID requirement and the other two deal with the requirement that new voters prove their U.S. citizenship the first time they register to vote.

1. Arthur Sprye and Charles Hamner v. Kris W. Kobach
In a suit filed November 1, 2013, two Osage County voters challenged the constitutionality of the photo ID requirement.

2. Kris W. Kobach, Kansas Secretary of State; and Ken Bennett, Arizona Secretary of State; v. United States Election Assistance Commission
In a suit filed in U.S. District Court in Kansas on August 21, 2013, the Kansas and Arizona Secretaries of State asked for a ruling to require the Election Assistance Commission to include the citizenship requirement in the voter instructions accompanying the universal federal voter registration application form, which is prescribed by the EAC. This lawsuit is in response to the June 17, 2013 ruling by the U.S. Supreme Court in Arizona v. Inter Tribal Council of Arizona regarding the constitutionality of states' requirements that voters provide proof of citizenship. The Court's ruling indicated that states might file suit if the EAC declined to make the necessary changes to the voter registration form administratively.

3. Aaron Belenky, Scott Jones, and Equality Kansas v. Kris Kobach, Kansas Secretary of State, and Brad Bryant, Kansas Elections Director
In a suit filed November 21, 2013, the plaintiffs seek declaratory and injunctive relief to keep the secretary of state's office from implementing a dual voter registration system. The SOS office had developed contingency plans to administer voter registration and ballots to individuals who attempted to register using the universal federal form but who had not provided proof of U.S. citizenship in compliance with Kansas law. No actions have been taken to implement the plan, and no federal elections have occurred in which federal-only ballots were administered to these voters. (See also Canvassing Kansas, September 2013, page 1.)

The goal of the secretary of state's office is to have the cases decided as soon as possible so CEOs and poll workers will know the rules before preparations begin for the 2014 election season. ■

Kobach Reappoints Lehman

Secretary of State Kris Kobach reappointed Tabitha Lehman as Sedgwick County Election Commissioner in September 2013. Her regular term expires on July 19, 2017. This will be Lehman's first full term as election commissioner, having been appointed to fill an unexpired term in 2011.

Lehman was appointed in November 2011 to succeed Bill Gale who resigned his position to pursue other employment. Gale had been appointed in November 2003 to succeed Marilyn Chapman, and he was reappointed in July 2009.

Speaking of her reappointment, Lehman said:
"I appreciate the opportunity to continue serving the voters of Sedgwick County and look forward to providing them with safe and efficient elections in the coming four years." ■

Sedgwick County Election Commissioner Tabitha Lehman
Photo courtesy of Tabitha Lehman

Crosscheck
Cont'd

Evidence of double votes is presented to law enforcement officers for investigation and possible prosecution. The referral is usually made to county law enforcement officers, but state or federal officials may be involved in some cases.

States join the crosscheck by signing a Memorandum of Understanding. The chief state election officer (usually the secretary of state) or a designee may sign the MOU for a given state.

Participating states pull their entire voter registration databases and upload them to a secure FTP site on January 15 each year. The Kansas SOS office IT staff pull the states' data from the FTP site, run the comparison, and upload each state's results to the FTP site. Each state then pulls its results from the FTP site and processes them according to its individual laws, regulations and procedures. In Kansas, results are provided to CEOs with instructions for analyzing them and mailing confirmation notices.

The crosscheck program is one of several list maintenance programs used to keep registration records up to date. (See also Canvassing Kansas, March 2010, page 9.) ■

Attorney General
Cont'd

If the governing body or chief administrative officer of a state or municipal building does not exempt a building from the provisions of K.S.A. 2013 Supp. 75-7c20, then concealed carry licensees must be permitted to carry a concealed handgun inside the building unless adequate security measures are provided and the building is posted as prohibiting concealed carry.

Concealed carry is not required to be permitted in a polling place located inside a privately-owned building unless the county has leased the entire privately-owned building.

Concealed carry is not required to be permitted in polling places located inside public school district buildings because a public school district is not a municipality for the purposes of the PFPA.

An equal protection claim against a county based upon the varying ability of concealed carry licensees to carry a concealed handgun into a polling place would be subject to the rational basis test. ■

Jury List Program Initiated

A 2013 law which went into effect July 1, 2013, requires district courts in Kansas to provide to the secretary of state the names of prospective jurors who indicate on their jury questionnaires that they are not United States citizens. Noncitizens are exempt from jury duty. The secretary of state passes the names on to CEOs for review. If they are found to be registered voters, their registrations are canceled. (See 2013 House Bill 2164; 2013 Kansas Session Laws Chapter 85.)

The relevant section of the law is New Section 1, reproduced below. Most of the bill deals with grand juries.

New Section 1. (a) On and after July 1, 2013, any jury commissioner that receives information regarding citizenship from a prospective juror or court of this state that disqualifies or potentially disqualifies such prospective juror from jury service pursuant to K.S.A. 43-156, and amendments thereto, shall submit such information to the secretary of state in a form and manner approved by the secretary of state. Any such information provided by a jury commissioner to the secretary of state shall be limited to the information regarding citizenship and the full name, current and prior addresses, age and telephone number of the prospective juror, and, if available, the date of birth of the prospective juror. Any such information provided by a jury commissioner to the secretary of state shall be used for the purpose of maintaining voter registrations as required by law.

The secretary of state's office worked with the Office of Judicial Administration (OJA) to design the following procedure to comply with the law:

- The clerk in each of Kansas' 31 judicial districts will submit a monthly report directly to the SOS office containing names of persons who were exempted from jury duty on the basis of their claims to be non-U.S. citizens.
- Reports will be submitted via email on or after the 15th of each month beginning in December 2013.
- The SOS will notify OJA of missing reports. OJA will contact any such district court clerks to remind them to submit their reports.
- If any of the persons listed in the reports are found to be registered voters and their citizenship status is not in doubt, their names will be sent by the SOS office to the appropriate county election officers with instructions regarding the possible cancellation of the persons' voter registration records. ■

18-F-1517//1087

State Fair Opinion Poll Results

The Office of the Secretary of State has operated a booth in the Meadowlark Building at the Kansas State Fair in Hutchinson for more than 25 years. The dates of the fair this year were September 6-15. This was the 100th anniversary of the fair, and the theme was "Never Gets Old."

At the booth, the SOS office provides information about agency activities, registers voters, and conducts an opinion poll on current issues. Don Merriman, Saline County Clerk, has assisted the SOS office for many years by lending ES&S iVotronic voting machines to help the fair visitors familiarize themselves with electronic voting technology. We want to recognize and thank Don for his assistance and the Lockwood Company for its donation of ballot programming services.

The SOS booth is mostly staffed by agency employees, but sometimes county election office personnel help out by volunteering to work in the booth. This year's county volunteers were: Sharon Seibel, Ford County Clerk; Debbie Cox, Ford County Deputy Clerk; Donna Maskus, Ellis County Clerk; Don Merriman, Saline County Clerk; Crysta Torson, Lane County Clerk; and Karen Duncan, Lane County Deputy Clerk. Thanks to the volunteers for helping out!

Following are the results of the opinion poll:

Question #1: New Kansas voters must provide proof of citizenship when registering to vote.

709 *I approve of this requirement.*
96 *I do not approve of this requirement.*
27 *I have no opinion about this requirement.*

Question #2: Which university will advance the furthest in the 2014 NCAA Men's Basketball Tournament?

397 *University of Kansas*
196 *Kansas State University*
179 *Wichita State University*
48 *None will make the tournament*

Question #3: Which of these alleged abuses of power by the federal government is the most concerning to you?

342 *NSA secretly collecting phone records of millions of U.S. citizens.*
332 *IRS intentionally discriminating against conservative organizations.*
153 *Presidential political appointees using secret email accounts to conduct official government business.*
132 *White House's sweeping seizure of Associated Press records and cable television documents.*

Question #4: Should the Internal Revenue Service be abolished?

526 *Yes. A flat or fair tax is simpler, cheaper and easier to manage.*
86 *Yes. We shouldn't have to pay income tax anyway.*
125 *No. Better training and oversight will fix most problems.*
2 *No. There is nothing wrong with the IRS.*

Question #5: Who is your favorite super hero?

90 *Xena: Warrior Princess*
379 *Superman*
94 *Wonder Woman*
195 *Batman* ■

Former Longtime Neosho County Clerk Dies

Wayne B. Gibson, Jr., a well known longtime county clerk from Neosho County, died on September 18, 2013, at a hospital in Labette County. Wayne served many years in the Neosho County Clerk's office and was known to Kansas election officials as a hardworking, conscientious public servant.

Gibson started working in the county clerk's office on January 16, 1961 and became Deputy Clerk about a month later. He then became Clerk on July 14, 1971, following the death of his predecessor, Virgil Lowe. Gibson served continuously until his retirement on April 20, 2007. During that time he was elected ten times - in 1972, 1974, 1976, 1980, 1984, 1988, 1992, 1996, 2000 and 2004.

The vacancy created by Gibson's resignation was filled by Randal Neely, who took office on August 1, 2007, and continues in office today. ■

Dominion Seeks Voting System Certification

Dominion Voting Systems, Inc., submitted a letter dated October 4, 2013 requesting certification of its Democracy Suite Version 4.14 voting system. According to Kansas law, a manufacturer seeking certification of its voting system must submit a formal letter, pay a $500 fee, and demonstrate the system at a certification hearing held in Topeka.

A hearing was held at the secretary of state's office on November 21, 2013, attended by Secretary of State Kris Kobach and members of his staff. The Democracy Suite system was demonstrated and explained by Norma Townsend, Don Vopalensky, Jeff Hintz and Michael Kelava. Dominion is represented in Kansas by its subcontractor, Election Source. Dominion also markets and services Premier (formerly Diebold) voting equipment, having purchased Premier from Election Systems and Software several years ago. ES&S still sells and services Premier equipment along with its own system, but Dominion owns the intellectual property rights of Premier equipment as a result of its purchase of the company.

As of this writing, Secretary Kobach has not certified the Dominion Democracy Suite. CEOs will be notified if and when certification is granted.

The Democracy Suite is a paper optical scan-based system which includes precinct ballot scanners and central scanners. The accessible ADA- and HAVA-compliant device allows a voter with a visual impairment to record his/her choices using an audio ballot and keypad. The system prints an optical scan ballot that is scanned along with other ballots. ■

Sedgwick County Sued Over Ballot Records

Sedgwick County Election Commissioner Tabitha Lehman was sued by a person seeking public access to Real Time Audit Logs (RTALs) on electronic voting machines. RTAL is ES&S's trade name for a voter verifiable paper audit trail (VVPAT), which is a printable electronic record of each voter's actions on the voting machine. RTAL documents are viewable by the voter before the electronic ballot is cast. Once the voter has cast the ballot the documents are randomly stored in the system's memory.

Elizabeth Clarkson v. Sedgwick County Elections Commissioner Tabitha Lehman was filed in state district court in Sedgwick County on June 18, 2013. The plaintiff sought access to RTAL records pursuant to the Kansas Open Records Act in order to conduct a post-election audit of the results of the November 2010 election.

In response to the plaintiff's original request for records, the election office provided precinct-based results tapes but denied the request for individual ballot logs, citing K.S.A. 25-2422 and the unnecessary burden and expense required to produce the records. State law does provide limited access to election records in a recount, but the law does not have specific provisions related to VVPATs or RTALs. These arguments were detailed in a response filed in court in July.

The court ruled in favor of the election commissioner's office. ■

SOS Holiday Hours

In observance of the regular calendar of state holidays, the secretary of state's office will be closed on the following dates:

December 25, 2013, for Christmas Day, and **January 1, 2014,** for New Year's Day.

In addition, the office will be closed Monday, **January 20, 2014** in observance of Martin Luther King, Jr. Day.

Happy Holidays from the SOS office!

18-F-1517//1089

Exhibit 34

Interstate Voter Registration Crosscheck Program

National Association of State Election Directors

January 26, 2013

Kris W. Kobach

18-F-1517//1091

National Voter Registration Act of 1993

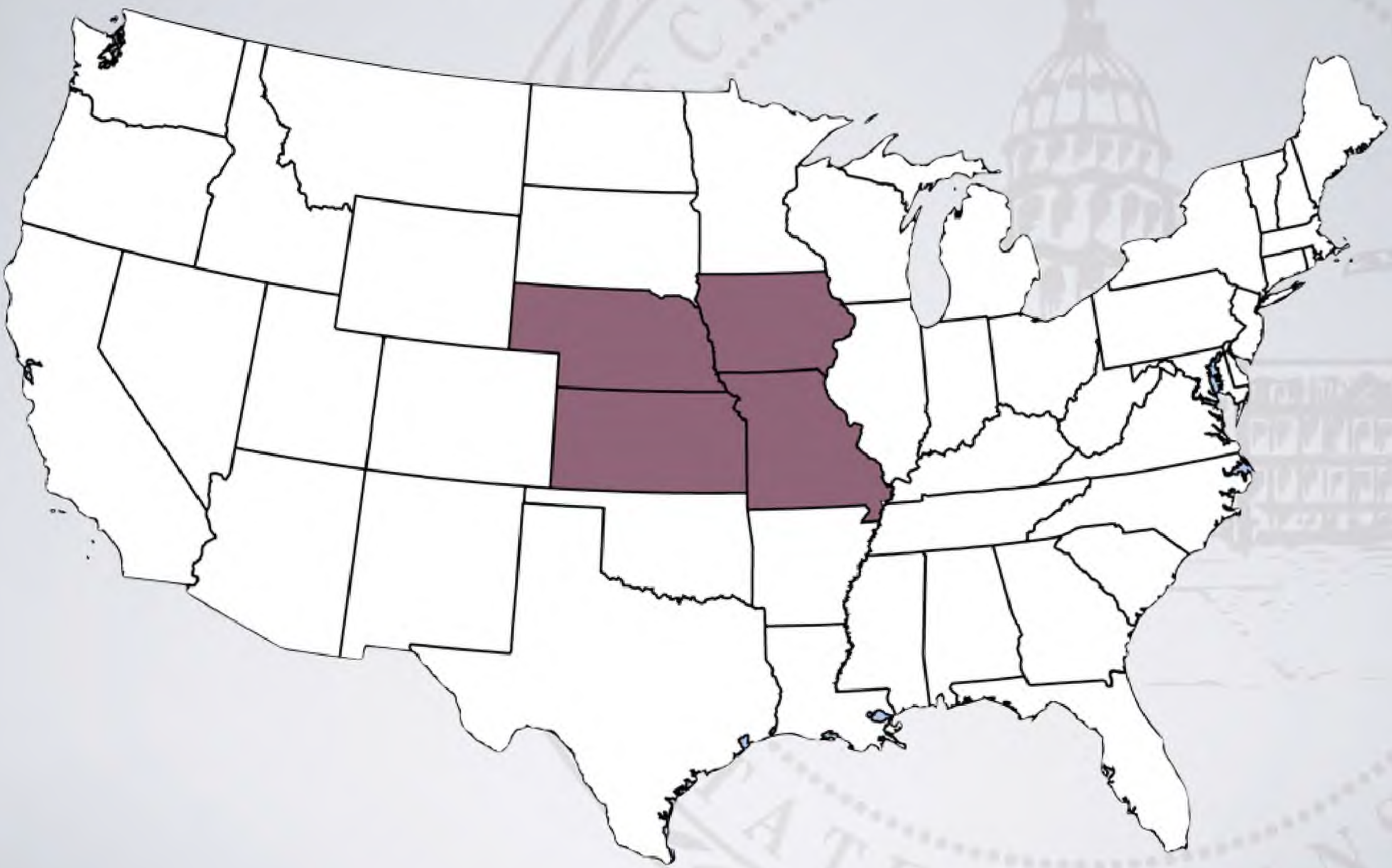
- **Section 2 Findings and Purposes**
- (b) Purposes
- (1) to establish procedures that will increase the number of eligible citizens who register to vote in elections for Federal office;
- (2) to make it possible for Federal, State, and local governments to implement this subchapter in a manner that enhances the participation of eligible citizens as voters in elections for Federal office;
- (3) to protect the integrity of the electoral process; and
- **(4) to ensure that accurate and current voter registration rolls are maintained.**

From the Federal Election Commission's guide: Implementing the National Voter Registration Act of 1993:

The features (of the National Voter Registration Act) include a requirement that states "conduct a general program" the purpose of which is "to protect the integrity of the electoral process by ensuring the maintenance of an accurate and current voter registration roll for elections for Federal office"

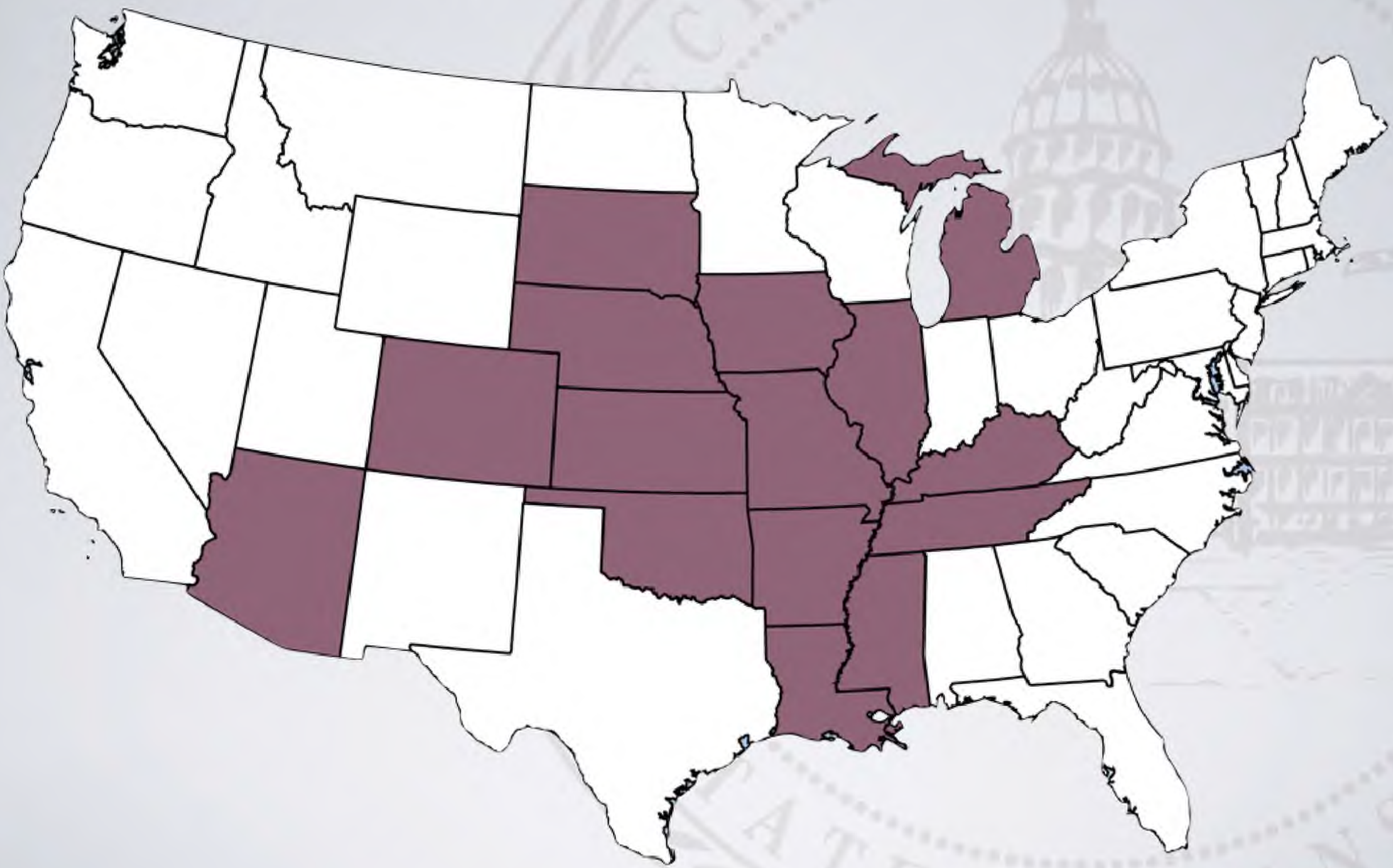
18-F-1517//1093

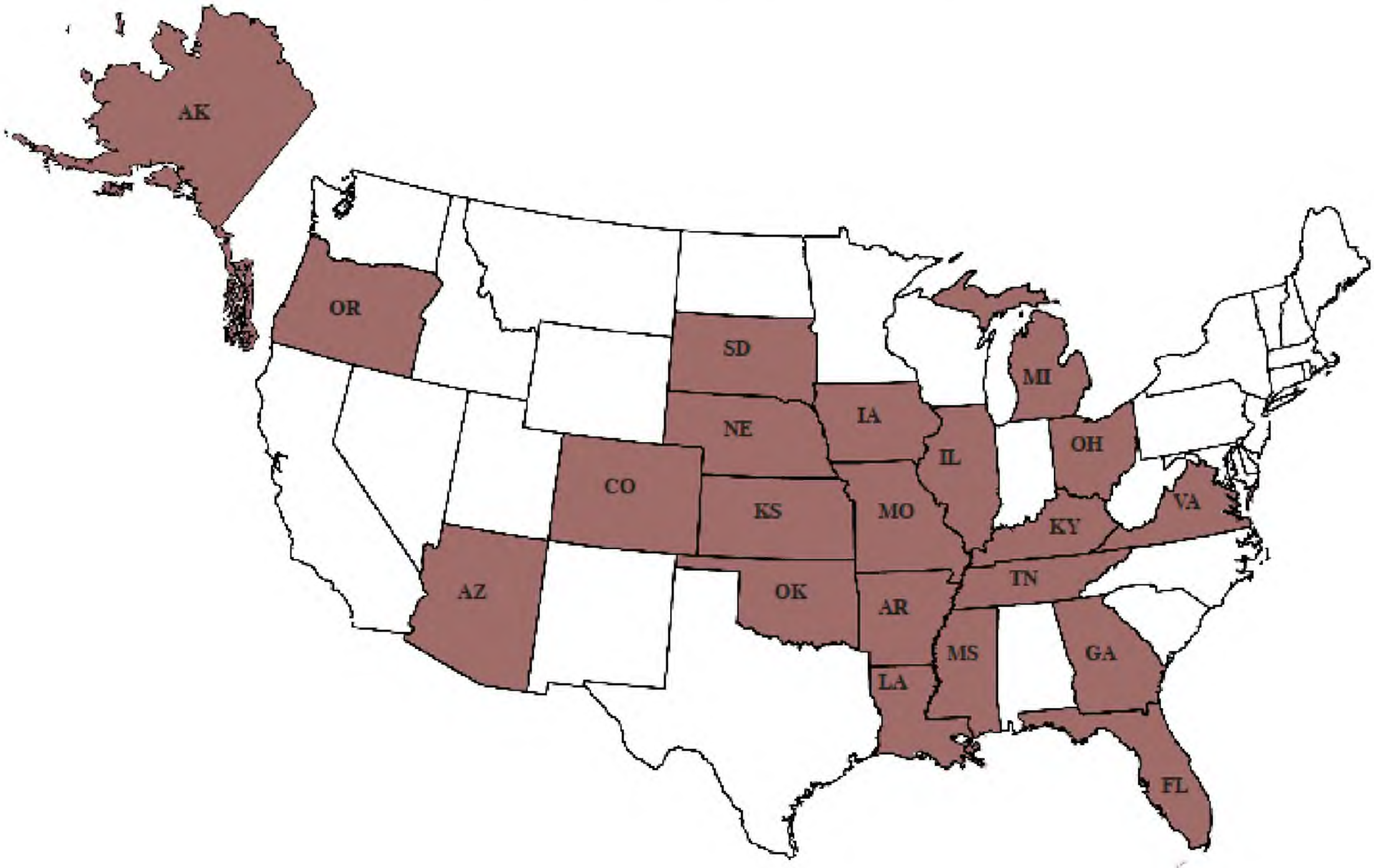
Participants in 2005



18-F-1517//1094

Participants in 2012





2013 Interstate Crosscheck

Participating states as of Jan. 10, 2013

18-F-1517//1096

2012 Crosscheck Program—Number of Records Compared

Arizona	3,545,891	Michigan	7,337,846
Arkansas	1,528,458	Mississippi	2,002,406
Colorado	3,375,891	Missouri	4,069,576
Illinois	8,248,736	Nebraska	1,129,943
Iowa	2,113,199	Oklahoma	2,000,767
Kansas	1,702,495	South Dakota	560,147
Kentucky	1,303,684	Tennessee	3,468,503
Louisiana	2,860,281		

Total Records: 45,247,823

18-F-1517//1097

Interstate Crosscheck Data Format

Field	Format	Example
Status	A=Active; I=Inactive	A
Date_Generated	YYYY/MM/DD	2010/01/01
First_Name		Bob
Middle_Name		Alan
Last_Name		Jones
Suffix Name		Jr
Date_of_Birth	YYYY/MM/DD	1940/06/16
Voter_ID_Number		123456
Last_4_SSN		7890
Mailing Address	Line 1 Line 2 City State Zip	123 Anywhere St...
County		Allen
Date_of_Registration	YYYY/MM/DD	1970/01/01
Voted_in_2010	Y=did vote; N=did not vote	Y

How does it work?

- Each state pulls data on January 15 each year using prescribed data format
- Upload data to secure FTP site (hosted by Arkansas)
- Kansas IT department pulls data, runs comparison, uploads results to FTP site
- Each state downloads results from FTP site, processes them according to state laws & regulations
- Kansas deletes all other states' data

18-F-1517//1099

First: John
Middle: Q.
Last: Public
DOB: 01/01/1975
SSN: 1234
State: Kansas

First: John
Middle:
Last: Public
DOB: 01/01/1975
SSN: 1234
State: Colorado

Potential match

Grid of Potential Duplicate Voters Within States

by DOB Last Name First Name

2012	AZ	AR	CO	IL	IA	KS	KY	LA	MI	MS	MO	NE	OK	SD	TN
AZ		2,829	24,863	16,014	7,153	3,687	688	2,062	27,617	2,220	7,569	3,306	4,006	2,449	3,614
AR	2,829		4,557	6,950	2,430	2,686	691	5,957	5,085	6,477	11,049	995	7,403	433	7,180
CO	24,863	4,557		19,902	10,850	10,035	1,054	5,065	17,086	3,309	12,498	8,927	8,306	3,937	6,153
IL	16,014	6,950	19,902		31,882	6,311	2,467	5,207	49,260	10,766	39,658	3,803	4,834	1,500	12,469
IA	7,153	2,430	10,850	31,882		4,706	526	1,558	7,019	1,797	11,563	10,954	2,031	4,865	2,806
KS	3,687	2,686	10,035	6,311	4,706		401	1,369	4,461	1,397	31,082	4,196	6,575	905	2,205
KY	688	691	1,054	2,467	526	401		873	2,267	1,085	1,195	233	576	117	1,905
LA	2,062	5,957	5,065	5,207	1,558	1,369	873		6,851	17,744	5,254	810	2,829	277	4,422
MI	27,617	5,085	17,086	49,260	7,019	4,461	2,267	6,851		7,527	12,960	2,416	4,067	1,265	16,956
MS	2,220	6,477	3,309	10,766	1,797	1,397	1,085	17,744	7,527		5,607	780	2,364	305	21,661
MO	7,569	11,049	12,498	39,658	11,563	31,082	1,195	5,254	12,960	5,607		4,244	7,539	1,300	7,804
NE	3,306	995	8,927	3,803	10,954	4,196	233	810	2,416	780	4,244		1,126	2,608	1,108
OK	4,006	7,403	8,306	4,834	2,031	6,575	576	2,829	4,067	2,364	7,539	1,126		402	2,858
SD	2,449	433	3,937	1,500	4,865	905	117	277	1,265	305	1,300	2,608	402		537
TN	3,614	7,180	6,153	12,469	2,806	2,205	1,905	4,422	16,956	21,661	7,804	1,108	2,858	537	
Totals	**108,077**	**64,722**	**136,542**	**211,023**	**100,140**	**80,016**	**14,078**	**60,278**	**164,837**	**83,039**	**159,322**	**45,506**	**54,916**	**20,900**	**91,678**

1317517.1101

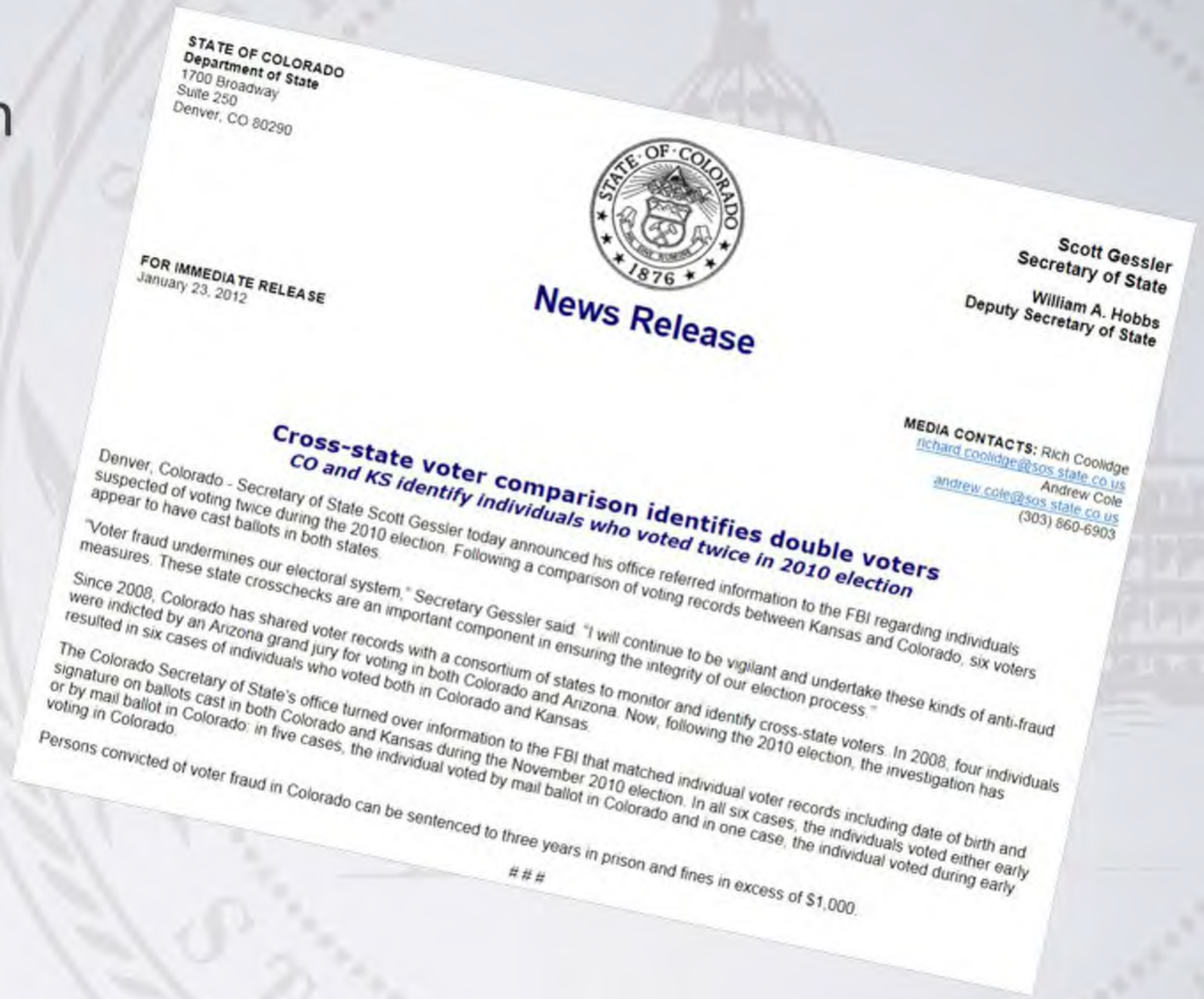
Success in Kansas

Double Votes from 2008 and 2010 Referred to Prosecution Discovered through Interstate Crosscheck Program	
2008	**2010**
Kansas - Kentucky	Kansas – Arkansas (2)
Kansas - Colorado	Kansas – Colorado (5)
Kansas - Kansas	Kansas – Iowa
	Kansas – Louisiana
	Kansas – Nebraska
	Kansas - Oklahoma

Kris W. Kobach

Success in other states - Colorado

- Four individuals indicted for voting in Colorado and Arizona in first year of participation
- Six additional cases of double voting referred to FBI in 2012



STATE OF COLORADO
Department of State
1700 Broadway
Suite 250
Denver, CO 80290

Scott Gessler
Secretary of State

William A. Hobbs
Deputy Secretary of State

FOR IMMEDIATE RELEASE
January 23, 2012

News Release

MEDIA CONTACTS: Rich Coolidge
richard.coolidge@sos.state.co.us
Andrew Cole
andrew.cole@sos.state.co.us
(303) 860-6903

Cross-state voter comparison identifies double voters
CO and KS identify individuals who voted twice in 2010 election

Denver, Colorado - Secretary of State Scott Gessler today announced his office referred information to the FBI regarding individuals suspected of voting twice during the 2010 election. Following a comparison of voting records between Kansas and Colorado, six voters appear to have cast ballots in both states.

"Voter fraud undermines our electoral system," Secretary Gessler said. "I will continue to be vigilant and undertake these kinds of anti-fraud measures. These state crosschecks are an important component in ensuring the integrity of our election process."

Since 2008, Colorado has shared voter records with a consortium of states to monitor and identify cross-state voters. In 2008, four individuals were indicted by an Arizona grand jury for voting in both Colorado and Arizona. Now, following the 2010 election, the investigation has resulted in six cases of individuals who voted both in Colorado and Kansas.

The Colorado Secretary of State's office turned over information to the FBI that matched individual voter records including date of birth and signature on ballots cast in both Colorado and Kansas during the November 2010 election. In all six cases, the individuals voted either early or by mail ballot in Colorado; in five cases, the individual voted by mail ballot in Colorado and in one case, the individual voted during early voting in Colorado.

Persons convicted of voter fraud in Colorado can be sentenced to three years in prison and fines in excess of $1,000.

###

Kris W. Kobach

What does it cost to participate?

$0

How Can a State Join the Crosscheck?

1. Chief State Election Official signs the Memorandum of Understanding (MOU)

2. CSEO assigns two staff members:
   - one election administration person
   - one IT person

3. Staff members will:
   - participate in annual conference call and email
   - pull VR data in January
   - receive cross check results and process
   - instruct local elections officials (respond to requests for addresses, signatures on poll books, etc.)

Contact

Brad Bryant
State Election Director
Kansas Secretary of State's Office
brad.bryant@sos.ks.gov
785-296-4561

Kris W. Kobach

Exhibit 35

The GOP's Stealth War Against Voters

Will an anti-voter-fraud program designed by one of Trump's advisers deny tens of thousands their right to vote in November?

The Crosscheck program is a response to the imaginary menace of mass voter fraud. Mark Makela/Reuters

By Greg Palast
August 24, 2016

When Donald Trump claimed, "the election's going to be rigged," he wasn't entirely wrong. But the threat was not, as Trump warned, from Americans committing the crime of "voting many, many times." What's far more likely to undermine democracy in November is the culmination of a decade-long Republican effort to disenfranchise voters under the guise of battling voter fraud. The latest tool: Election officials in more than two dozen states have compiled lists of citizens whom they allege could be registered in more than one state – thus potentially able to cast multiple ballots – and eligible to be purged from the voter rolls.

The data is processed through a system called the Interstate Voter Registration Crosscheck Program, which is being promoted by a powerful Republican operative, and its lists of potential duplicate voters are kept confidential. But *Rolling Stone* obtained a portion of the list and the names of 1 million targeted voters. According to our analysis, the Crosscheck list disproportionately threatens solid Democratic constituencies: young, black, Hispanic and Asian-American voters – with some of the biggest possible purges underway in Ohio and North Carolina, two crucial swing states with tight Senate races.

RELATED

18-F-1517//1108

2016: First Presidential Election Since Voting Rights Gutted

America will vote for president in a country where it's easier to buy a gun than vote in many states

Like all weapons of vote suppression, Crosscheck is a response to the imaginary menace of mass voter fraud. In the mid-2000s, after the Florida-recount debacle, the Bush administration launched a five-year investigation into the allegedly rampant crime but found scant evidence of wrongdoing. Still, the GOP has perpetuated the myth in every national election since. Recently, North Carolina Board of Elections chief Kim Strach testified to her legislature that 35,750 voters are "registered in North Carolina and another state and voted in both in the 2012 general election." [Editor's note: This quote was taken from the power point that accompanied Strach's testimony. In a subsequent letter, she informed us that during her presentation she "stressed that we were not suggesting that 35,750 voters had committed any type of fraud. My testimony was that the data we received from the Crosscheck Program showed that in the 2012 general election, there were 35,750 people who voted in North Carolina whose first and last names and dates of birth matched persons who voted in the same election in another state."] Yet despite hiring an ex-FBI agent to lead the hunt, the state has charged exactly zero double voters from the Crosscheck list. Nevertheless, tens of thousands face the loss of their ability to vote – all for the sake of preventing a crime that rarely happens. So far, Crosscheck has tagged an astonishing 7.2 million suspects, yet we found no more than four perpetrators who have been charged with double voting or deliberate double registration.

On its surface, Crosscheck seems quite reasonable. Twenty-eight participating states share their voter lists and, in the name of dispassionate, race-blind Big Data, seek to ensure the rolls are up to date. To make sure the system finds suspect voters, Crosscheck

supposedly matches first, middle and last name, plus birth date, and provides the last four digits of a Social Security number for additional verification.

In reality, however, there have been signs that the program doesn't operate as advertised. Some states have dropped out of Crosscheck, citing problems with its methodology, as Oregon's secretary of state recently explained: "We left [Crosscheck] because the data we received was unreliable."

In our effort to report on the program, we contacted every state for their Crosscheck list. But because voting twice is a felony, state after state told us their lists of suspects were part of a criminal investigation and, as such, confidential. Then we got a break. A clerk in Virginia sent us its Crosscheck list of suspects, which a letter from the state later said was done "in error."

The Virginia list was a revelation. In all, 342,556 names were listed as apparently registered to vote in both Virginia and another state as of January 2014. Thirteen percent of the people on the Crosscheck list, already flagged as inactive voters, were almost immediately removed, meaning a stunning 41,637 names were "canceled" from voter rolls, most of them just before Election Day.

We were able to obtain more lists – Georgia and Washington state, the total number of voters adding up to more than 1 million matches – and Crosscheck's results seemed at best deeply flawed. We found that one-fourth of the names on the list actually lacked a middle-name match. The system can also mistakenly identify fathers and sons as the same voter, ignoring designations of Jr. and Sr. A whole lot of people named "James Brown" are suspected of voting or registering twice, 357 of them in Georgia alone. But according to Crosscheck, James Willie Brown is supposed to be the

18-F-1517//1110

same voter as James Arthur Brown. James Clifford Brown is allegedly the same voter as James Lynn Brown.

And those promised birth dates and Social Security numbers? The Crosscheck instruction manual says that "Social Security numbers are included for verification; the numbers might or might not match" – which leaves a crucial step in the identification process up to the states. Social Security numbers weren't even included in the state lists we obtained.

We had Mark Swedlund, a database expert whose clients include eBay and American Express, look at the data from Georgia and Virginia, and he was shocked by Crosscheck's "childish methodology." He added, "God forbid your name is Garcia, of which there are 858,000 in the U.S., and your first name is Joseph or Jose. You're probably suspected of voting in 27 states."

Swedlund's statistical analysis found that African-American, Latino and Asian names predominate, a simple result of the Crosscheck matching process, which spews out little more than a bunch of common names. No surprise: The U.S. Census data shows that minorities are overrepresented in 85 of 100 of the most common last names. If your name is Washington, there's an 89 percent chance you're African-American. If your last name is Hernandez, there's a 94 percent chance you're Hispanic. If your name is Kim, there's a 95 percent chance you're Asian.

The Crosscheck program, started by Kris Kobach, has spread to over two dozen states, tagging more than 7 million voters as possibly suspect. Christopher Smith/Washington Post/Getty

This inherent bias results in an astonishing one in six Hispanics, one in seven Asian-Americans and one in nine African-Americans in Crosscheck states landing on the list. Was the program designed to target voters of color? "I'm a data guy," Swedlund says. "I can't tell you what the intent was. I can only tell you what the

18-F-1517//1111

outcome is. And the outcome is discriminatory against minorities."

Every voter that the state marks as a legitimate match receives a postcard that is colorless and covered with minuscule text. The voter must verify his or her address and mail it back to their secretary of state. Fail to return the postcard and the process of taking your name off the voter rolls begins.

This postcard game amplifies Crosscheck's built-in racial bias. According to the Census Bureau, white voters are 21 percent more likely than blacks or Hispanics to respond to their official requests; homeowners are 32 percent more likely to respond than renters; and the young are 74 percent less likely than the old to respond. Those on the move – students and the poor, who often shift apartments while hunting for work – will likely not get the mail in the first place.

At this point, there's no way to know how each state plans to move forward. If Virginia's 13 percent is any indication, almost 1 million Americans will have their right to vote challenged. Our analysis suggests that winding up on the Crosscheck list is hardly proof that an individual is registered in more than one state. Based on the data, the program – whether by design or misapplication – could save the GOP from impending electoral annihilation. And not surprisingly, almost all Crosscheck states are Republican-controlled.

The man behind crosscheck is Kansas Secretary of State Kris Kobach, a Yale-educated former law professor. After 9/11, U.S. Attorney General John Ashcroft tasked Kobach with creating a system to track foreign travelers. (It was later shut down over concerns about racial profiling.) He is best known as the author of Arizona's "Driving While Brown Law," which allowed cops to pull over drivers and ask for proof of their legal status. He co-wrote the ultraconservative 2016 RNC

18-F-1517//1112

party platform, working in a recommendation that Crosscheck be adopted by every state in the Union. He's also the Trump adviser who came up with a proposal to force Mexico into paying for Trump's wall.

In January 2013, Kobach addressed a gathering of the National Association of State Election Directors about combating an epidemic of ballot-stuffing across the country. He announced that Crosscheck had already uncovered 697,537 "potential duplicate voters" in 15 states, and that the state of Kansas was prepared to cover the cost of compiling a nationwide list. That was enough to persuade 13 more states to hand over their voter files to Kobach's office.

In battleground-state Ohio, Republican Secretary of State John Husted's Crosscheck has flagged close to half a million voters. In Dayton, we tracked down several of the suspects on our lists. Hot spots of "potential duplicate" voters, we couldn't help but notice, were in neighborhoods where the streets are pocked with rundown houses and boarded storefronts. On Otterbein Avenue, I met Donald Webster, who, like most in his neighborhood, is African-American.

Crosscheck lists him registered in Ohio as Donald Alexander Webster Jr., while registered a second time as Donald *Eugene*Webster (no "Jr.") in Charlottesville, Virginia. Webster says he's never been a "Eugene" and has never been to Charlottesville. I explained that both he and his Virginia doppelgänger were subject to losing their ability to vote.

"How low can they go?" he asked. "I mean, how can they do that?"

I put his question to Robert Fitrakis, a voting-rights attorney who examined our Crosscheck data. I showed him Donald Webster's listing – and page after page of Ohio voters. Fitrakis says that the Ohio secretary of state's enthusiasm for Crosscheck fits a pattern: "He

doesn't want to match middle names, because he doesn't want real matches. They're targeting people with clearly defined ethnic names that typically vote for the Democratic Party. He wants to win Ohio the only way he knows how – by taking away the rights of citizens to vote."

Kobach refused to speak for this story. So I went to Newton, Kansas, where he was headlining an ice-cream-social fundraiser in a public park. I approached Kobach with the Crosscheck list he had refused me, and asked, "Why are these lists so secret?"

RELATED
Watch John Oliver's Takedown of Voter ID Laws
"It's just one of those things that white people are more likely to have. Like a sunburn. Or an Oscar nomination," host says of IDs

"They aren't," Kobach answered, contradicting what his attorney had told me.

I pointed to a random match on the Crosscheck list and asked him why it identified James *Evans* Johnson as the same voter as James P. Johnson.

Kobach denied the name could be on the list. "Our system would not yield this match," he said. (And according to the rules of his program, it shouldn't have.)

"This is the list you gave [Virginia], and they knocked off 41,000 voters," I said.

"That is false!" he said, as he hurried away. "You know why? Federal law prohibits that."

Kobach is correct that federal regulation typically would complicate such a sweeping purge, but somehow tens of thousands of voters in Virginia got knocked off the rolls anyway.

Kobach's Crosscheck purge machinery was in operation well before Trump arrived on the political scene – and will continue for elections to come. Low voter turnout of any kind traditionally favors the GOP, and this is the party's long game to keep the rolls free of young people, minorities and the poor. Santiago Juarez of New Mexico, an attorney who has done work for the League of United Latin American Citizens, has spent years signing up Hispanic voters in the face of systemic efforts to suppress their vote. He scoffed at the idea of a massive conspiracy among Latinos to vote in two states. "Hell," he said, "you can't get people to vote once, let alone twice."

18-F-1517//1115

Exhibit 36

Report to Congress – December 2016

18-F-1517//1117

Table of Contents

18-F-1517//1118

Section 1

Introduction

18-F-1517//1119

In August 2014, the United States Digital Service (USDS) was created to improve the Federal Government's most important public-facing digital services. USDS is a collaboration between some of the country's top technical talent and the government's brightest civil servants, who work in partnership to apply private sector best practices to our digital services.

Initially, USDS' small team of technologists planned to focus on three projects. Additional funding and the support of Congress for the Information and Technology Oversight and Reform (ITOR) Fund in the 2015 and 2016 Fiscal Year appropriations bills allowed USDS to invest in a greater number of high-priority projects, detailed in this report. Of the $30M appropriated in the 2016 fiscal year, $14M was apportioned to USDS to support its operations, with the balance of the $30M supporting other IT oversight and reform activities. At its creation, USDS was administratively placed within the Office of the Federal CIO. After more than two years of operations, however, the Office of Management and Budget (OMB) has decided to move the Administrator of USDS to directly report to the Deputy Director of Management (DDM).

USDS staff in OMB work alongside agency Digital Service team staff to support high-priority projects in agencies including the Departments of Veterans Affairs, State, Education, Homeland Security, Health and Human Services, Defense, the Internal Revenue Service, and the Small Business Administration.

The central focus of USDS is on the measurable improvement of the performance and cost-effectiveness of important, public-facing Federal Government digital services – via the application of modern technology best practices. To execute this mission, USDS conducts hands-on engagements with agencies. A summary of USDS' most impactful engagements is provided in Section 2.

In support of its core mission of improving the performance and cost-effectiveness of important government digital services, the USDS engages in three additional activities:

- **Rethink how we build and buy digital services.** USDS is working on modernizing procurement processes and practices for the modern digital era. Our partners in the IT contracting community are a critical element of modernizing our government, as skilled contractors deliver the majority of the government's digital services.
- **Expand the use of common platforms, services and tools.** USDS is working with agencies to identify and implement shared tools and services to address common technical issues and usability challenges across the Federal Government. One example is building Login.gov, a universal login system that will enable the

18-F-1517//1120

American public to access multiple government agency services with one, streamlined account.

- **Bring top technical talent into public service.** In support of these goals, USDS has recruited and placed over 200 Digital Service Experts, from one of the most competitive industries in the world, to join the government for term-limited tours of duty with the USDS and work with civil servants inside agencies. The long-term goal is to encourage a tradition of public service in the tech industry that will support the ongoing improvement of government digital services.

USDS has developed procedures and criteria for prioritizing projects, which includes obtaining input from OMB's IT Dashboard, agency leadership, and relevant U.S. Government Accountability Office (GAO) reports. To prioritize projects, USDS also uses the following three criteria, which are listed in their order of importance:

(1) What will do the greatest good for the greatest number of people in the greatest need?
(2) How effective and cost-efficient will the USDS investment be?
(3) What potential exists to use or reuse a technological solution across the Federal Government?

Along with its investment in the ITOR Fund, Congress asked USDS to provide a regular update on progress in each of its programs. This report details that progress.

Mikey Dickerson
Administrator, U.S. Digital Service

18-F-1517//1121

Section 2

High Priority Projects

18-F-1517//1122

Priority Project Summary

USDS executes focused, hands-on engagements in which small teams of technical experts embed into existing agency programs, where they accelerate adoption of modern private sector best practices on important projects. These engagements may be proactive or reactive, and can range from two-week diagnostic sprints to in-depth multi-month engagements to dramatically improve a target service.

Typically, USDS is focused on increasing the success rate of a major IT acquisition in an agency. USDS personnel help promote the critical factors underlying successful major IT acquisitions identified by GAO in 2011 and reiterated in 2015 by GAO in its report on "Improving the Management of IT Acquisitions and Operations."

This section details USDS' most impactful projects, including those completed during the 2016 Fiscal Year:

- **Stabilizing and Improving HealthCare.gov (page 9).** In the 2013-2014 Open Enrollment season, a small team of private sector experts helped overhaul, update, and simplify the design and infrastructure of HealthCare.gov, helping eight million Americans sign up for coverage. This success paved the way for the creation of USDS. In the two subsequent open enrollment periods, USDS staff continued to partner with CMS staff and contractors to further improve the HealthCare.gov system and services.
- **Modernizing the Immigration System at DHS (page 14).** Since 2014, USDS has been helping USCIS implement private sector best practices on the Electronic Immigration System project. As of September 2016, 25% of immigration transactions applications are processed electronically using the system, including the green card renewal application (I-90), which has a 92% user satisfaction rate.
- **Streamlining VA Disability Claim Processing (page 20).** Over the summer of 2016, the USDS team at VA helped launch Caseflow Certification, a tool to improve paperless appeals processing by detecting if required documentation has been added before an appeal can move forward. This simple check helps reduce preventable errors and avoidable delays caused by disjointed, manual processing. As of September 2016, approximately 87% of all paperless appeals are certified using the tool.
- **Simplifying Veteran-facing Services with Vets.gov (page 26).** USDS is working with leaders across VA to build Vets.gov, a simple, easy-to-use site that consolidates information for Veterans. Over the summer, the USDS team helped VA launch a new digital application for healthcare built with feedback from

18-F-1517//1123

Veterans. Previously, less than 10 percent of applicants applied online. Since the launch of the new healthcare application, daily online applications have increased from 62 per day to more than 500 per day.

- **Providing Secure Access to IRS Taxpayer Information (page 31).** USDS helped IRS introduce Secure Access in June 2016, a user verification process that relies on strong identity proofing and two-factor authentication to protect users' sensitive tax records. Secure Access ensures that users have convenient, real-time access to their transcripts while protecting taxpayer information from automated fraudulent attacks. As of September 2016, taxpayers have accessed 2.7 million tax records using the Secure Access process.
- **Improving the Visa Processing System at Department of State (page 37).** USDS is assisting State to implement improvements in the Consolidated Consular Database, on which many Visa processing applications depend. USDS helped State adopt modern engineering best practices, and is helping State develop tools to communicate case status to applicants, which is the primary reason for many of the 9,000 phone calls the National Visa Center receives per day.
- **Helping CMS Implement Congressionally Mandated Medicare Payment Changes (page 41).** Implementation of the Medicare Access and Chip Reauthorization Act of 2015 (MACRA) will change the way Medicare pays doctors for services rendered to Medicare patients. USDS is helping CMS use modern best practices to ensure the transition from the current payment program to the new system is simple, clear and effective.
- **Reducing Inefficiency in the Refugee Admission Process (page 44).** Each year, the United States admits tens of thousands of refugees using a rigorous approval process. Previously, DHS officers had to approve refugee registration forms using an ink approval stamp in the field where the refugee file was physically located. USDS helped DHS and State implement a "digital stamp," removing an unnecessary processing delay of 2 to 8 weeks for thousands of cases.
- **Helping Students Make More Informed College Choices at Department of Education (page 49).** USDS, along with 18F, helped the Department of Education launch the College Scorecard to help students make more informed decisions about college selection. Millions of students have already benefited from this data, the most comprehensive and reliable ever published on employment outcomes and success in repaying student loans. Additionally, more than a dozen organizations have built new tools using the data.
- **Modernizing the Department of Defense Travel System (page 55).** The USDS team at DoD (Defense Digital Service) is helping implement a new commercial

18-F-1517//1124

tool to better manage the $3.5 billion of travel handled through the Defense Travel System each year.

- **Identifying Security Vulnerabilities in Department of Defense Websites (page 59).** To strengthen data security at DoD, the USDS team at DoD (Defense Digital Service) launched "Hack the Pentagon," the first bug bounty program in the history of the Federal Government. Adopting this private sector best practice led to the resolution of 138 previously unidentified vulnerabilities and cost $150,000, compared to the $1 million DoD estimates contracting an outside firm to do a similar audit would have cost.

Additional detail on each of these projects is provided in the chapters below.

18-F-1517//1125

Stabilizing and Improving HealthCare.gov

The Challenge

As required by the Affordable Care Act, HealthCare.gov is the Federal website that facilitates purchase of private health insurance for consumers who reside in states that did not establish health insurance marketplaces. HealthCare.gov supports the Federal Health Insurance Marketplace (Marketplace), providing citizens with the ability to compare, shop for, and enroll in affordable healthcare plans.

HealthCare.gov launched in October 2013, and encountered serious technical challenges which prevented many people from using the service.

Project Impact Summary

- A team of private sector engineers and product managers joined CMS staff and contractors to identify and solve website operation problems. By March 2014, over 8 million Americans had successfully signed up for health insurance and the site was stable.
- In the two subsequent open enrollment periods, USDS staff continued to partner with CMS to improve the HealthCare.gov system and services. USDS staff helped CMS implement several private sector best practices including performance tracking of the system and application process, building an improved identity management solution with an uptime of 99.99%, increasing the conversion rate in the new application workflow from 55% to 85%, and building new systems with industry standard open source software.

The Solution

Over the three month period following the launch, a team of engineers and product managers from the private sector joined with CMS staff and existing contractor teams to troubleshoot the service. Working around the clock, this "tech surge" team systematically identified and solved problems with the service by following industry best practices in site reliability and product management. By March 2014, the end of the Marketplace's first open enrollment period, over 8 million Americans had successfully signed up for health insurance.

The HealthCare.gov turn-around demonstrated the enormous potential of empowering small teams of America's brightest digital talent to apply modern technology best

18-F-1517//1126

practices to Federal Government projects. In August 2014, the White House established the U.S. Digital Service (USDS) to apply this technique to a greater number of projects. Mikey Dickerson, a site reliability engineer on the HealthCare.gov team, was appointed the USDS Administrator.

In the two subsequent open enrollment periods (ending February 2015 and January 2016), USDS engineers, product managers and designers partnered with CMS staff to continue to improve HealthCare.gov systems and processes used to deliver the service.

For example, contractors from multiple companies along with CMS staff improved coordination in the Healtchare.gov operations center by embracing a "one-team" mentality with fewer process restrictions, which has improved the ability of this team to troubleshoot issues and make important decisions quickly. The team also implemented application monitoring to track performance.

Additionally, USDS supported several smaller teams working on components of HealthCare.gov which adopted agile and iterative development processes, allowing them to quickly deliver functioning software. In one such case, a small team built and launched the Scalable Login System (SLS), a replacement for HealthCare.gov's previous identity management solution. SLS has proven to be vastly more stable and efficient since it was created specifically for use by Marketplace consumers.

18-F-1517//1127

Additionally, CMS launched a simpler and more efficient application for healthcare plan enrollment (Marketplace Lite 2.0 App). The conversion rate in the new application workflow stands at around 85%, compared with approximately 55% in the previous system. Finally, CMS with input from the insurer community, built and launched a new set of decision support tools for the window shopping and plan compare tools. These tools allow consumers to search for preferred doctors, prescription drugs, and facilities while shopping for a health plan. This was one of the most requested features from Marketplace consumers over the past several years.

Success Criteria	Status
Transition HealthCare.gov to a scalable login system with an uptime of 99% or greater	Complete. Scalable Login System implemented and users migrated to the system in 2015. Uptime 99.99%
Implement application monitoring.	Complete. Monitoring installed and in use.
Launch the Marketplace Lite 2.0 app	Complete. App launched in 2015, resulting in improved conversion rates.

Milestones

- October 2013: HealthCare.gov launches. "Tech surge" assists with troubleshooting the service.
- March 2014: First open enrollment period closes with 8 million Americans enrolled (5.3 million through HealthCare.gov).
- August 2014: USDS created.
- November 2014: Second open enrollment period begins. USDS team supports Marketplace operations.
- February 2015: Second open enrollment period ends with 11.7 million enrollments (8.8 million through HealthCare.gov). USDS team supports Marketplace operations and assists with the transition from to SLS.
- November 2015: Third open enrollment period begins. USDS team supports Marketplace operations
- January 2016: Third open enrollment period ends with 12.7 million enrollments (9.6 million through HealthCare.gov). USDS support role winds down.

18-F-1517//1128

The Process and Lessons Learned

1. **Install application monitoring.** At initial launch of HealthCare.gov, there was no end-to-end monitoring of the production system, making identification, prioritization and diagnosis of errors very challenging. One of the first actions the "tech surge" team took was to recommend the addition of an application monitoring tool, which has remained an important resource for the team to identify issues as they occur.

2. **Facilitate open and direct communication between technical contributors.** HealthCare.gov has many components, many of which were created by different companies hired by CMS. Problems with the integration of these components was a source of many errors in the initial launch. The most effective solution was to bring individual technical contributors from these various teams to a single location where problems could be discussed openly, solutions could be explored, and assignments could be made. Additionally, all staff and contractors working on aspects of HealthCare.gov began to use a collaboration tool to communicate more effectively.

3. **Deploy in a flexible hosting environment.** Traffic on HealthCare.gov is highly variable. Near the end of an enrollment period, for example, the number of visitors can increase by an order of magnitude.

   Several of the newer components of HealthCare.gov are deployed in a flexible cloud hosting environment (including SLS and the Marketplace Lite App 2.0 described above). CMS has experienced high availability and increased development speeds with this approach, and is seeking to use this approach for more of its components.

4. **Build services using agile and iterative processes.** CMS has had success using small teams to incrementally deliver enhanced functionality based on an evolving understanding of user needs. For example, the Marketplace Lite App 2.0 continues to be iteratively improved based on user feedback and metrics.

5. **Choose a modern technology stack.** The Scalable Login System was built with industry standard open source software components commonly used by the private sector. The service is deployed in the public commercial cloud. These decisions enabled the team to build the service at a lower cost.

18-F-1517//1129

Modernizing the Immigration System at DHS

The Challenge

Every year, the Department of Homeland Security's U.S. Citizenship and Immigration Services (USCIS) processes millions of immigration requests. This system is mostly paper-based, consists of multiple forms, and results in long waiting periods for applicants who have little visibility into the status of their applications.

USCIS wanted to modernize the process. They wanted a streamlined experience that would allow applicants to identify which form was meant for their specific situation, and enable adjudicators to process applications more efficiently and effectively than on paper.

To achieve this goal, USCIS began a five-year engagement with a technology vendor to create the Electronic Immigration System (ELIS). The project ran into a host of issues: the project scope was too large, the proprietary technology adopted was too complex and inflexible, and releases happened years after the project began. The agency was heavily reliant on specific vendors and proprietary technologies that proved costly and difficult to customize to address USCIS' product requirements.

ELIS fell short of expectations and didn't meet user needs – so USCIS made the hard but correct decision to restart the project using a new management style and a new technical approach that took key plays from private industry.

In 2014, members of the USDS joined the USCIS team to help the agency implement these changes, and the USDS has provided ongoing support to the agency since then.

Project Impact Summary

- Every year, USCIS processes millions of immigration requests. Its multi-year project to modernize this process (the ELIS project) ran into a host of issues common in Federal Government IT projects, leading USCIS to restart the project.
- In 2014, USDS staff engineers, designers and product managers began working with USCIS to help it implement private sector IT management best practices including agile software development and continuous integration.
- In March 2015, following a November 2014 soft launch, USDS supported USCIS with the release of online filing and adjudication of the Form I-90, the application to replace permanent resident cards. 92% of online I-90 filers (renewing or replacing their green cards) reported being satisfied with the experience.

18-F-1517//1130

- In February 2015, USCIS partnered with 18F, private contractors, and USDS to launch myUSCIS, a new service to help applications and their representatives better navigate the immigration process.
- The Immigrant Fee payment launched in August 2015, enabling over 1.1 million applicants to make fee payments digitally.
- USCIS has adopted deployment approaches that allow it to release improvements to ELIS weekly, compared to the quarterly release schedule the project followed previously.
- Today, 25% of immigration applications are processed electronically and USDS continues to work with USCIS to increase this percentage.

The Solution

In restarting the project, USCIS leadership changed the way they did business.

The team embraced an agile, iterative style of product development that allowed the agency to design, build and deploy functionality more quickly to respond to user needs. While the previous project had taken years before an initial launch, the new approach led to a beta release just one year after development began. Agency staff are now heavily involved in the day-to-day development effort, running stand-up meetings and increasing visibility across the team. Seasoned USDS product managers, engineers and designers partnered with the USCIS team to integrate these modern digital service practices.

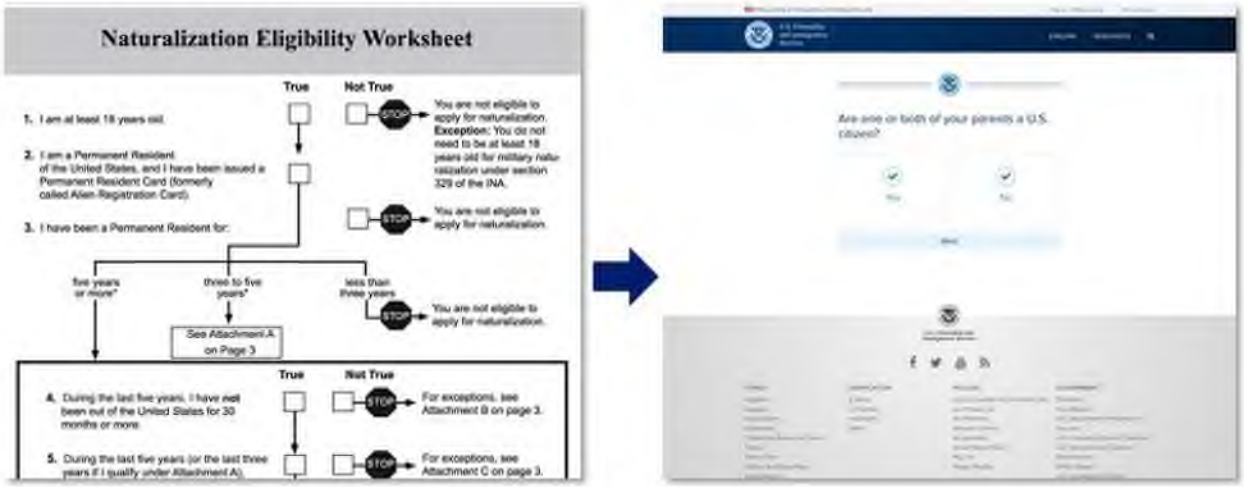
In order for the team to effectively support this agile development style, USCIS had to change its approach to contracting. They engaged with multiple vendors instead of using one large contract with a single vendor. The teams worked together to deliver features, build and maintain the infrastructure for the service, and enable the continuous integration of new improvements into the production system. The contracts are designed to support frequent prototyping, refining of product requirements, and delivery of working software. Most of them give USCIS the flexibility to ramp up or down the number of development teams from each vendor based on that vendor's performance.

USCIS also conducted deep research on their customers that led them to re-imagine the end-to-end immigrant experience well beyond the core actions of filing and processing requests. They began to redesign the immigrant experience around people, not form numbers.

In partnership with 18F and private contractors, USCIS brought this vision to life by launching myUSCIS, a new service built to help applicants and their representatives.

18-F-1517//1131

myUSCIS allows visitors to determine which immigration options are available to them, with a search-driven, plain-language knowledge base of direct answers to common immigration questions. It also now allows immigrants to apply for naturalization, make fee payments, provide supporting evidence, and look up their case status online.



Finally, USCIS technical leaders also made important changes to the architecture of ELIS. The development team has adopted many modern software development practices drawn from the private sector, including the use of open source software components, flexible deployment environments, and real-time monitoring. The team also continuously integrates changes to the system, using modern deployment and testing processes and tools. USCIS is implementing the "DevOps" model, in which there is no separation between development and operations teams.

These improvements in software development practices, design and system architecture are making it easier for users to interact with our immigration system. The team has hit several important milestones, including the release of online filing and adjudication of the Form I-90 (application to replace permanent resident card). USCIS has also begun to electronically process applications for naturalization. USCIS will continue to bring more parts of the immigration process into the new digital system and improve its processes around design, high-quality delivery, and system monitoring and response.

USDS will remain involved with the project to assist with delivery, design and operations.

18-F-1517//1132

Success Criteria	Status
Increased percentage of immigration applications processed electronically	In progress. 25% of immigration applications are now processed electronically
Increased customer satisfaction rating over time	In progress. 92% of online I-90 filers (renewing or replacing their green cards) reported being satisfied with the experience.
Increase frequency of ELIS releases	Complete. ELIS releases new code weekly, up from previous quarterly releases

Milestones

- July 2014: A "pilot" USDS engagement prior to its official launch in August began with a "Discovery Sprint" focused on ELIS
- November 2014: ELIS2 I-90 Three-Day "Soft" Launch
- March 2015: ELIS2 I-90 Full Launch
- August 2015: Immigrant Fee payment launched
- April 2016: ELIS2 Naturalization Pre-processing Go-live Date

The Process and Lessons Learned

1. **Understand what people need.** The USDS team helped USCIS implement a user-centered design process to ensure that the delivery team understood what people need the service to offer. USDS coordinated and led visits to field offices and the National Benefit Center to conduct direct observation of application processing, giving insight into users' needs and experiences. This user research informed the design of the system. The team further refined these designs by getting adjudicator feedback on simple mockups of functionality, and testing early versions of the system with adjudicators.

2. **Build services using agile and iterative practices.** In the new system, USCIS chose two high-volume services and focused on rapidly digitizing them using an

18-F-1517//1133

agile development process. The Form I-90 application to replace a permanent resident card was first launched in November 2014, and USCIS Immigrant Fee Payment launched in August 2015. These services were rolled out in an incremental manner, and teams continue to deliver bug fixes and enhancements on a weekly basis. The teams collect feedback from end users and engage in regular usability testing to identify opportunities to improve efficiency and inform development of future product lines.

3. **Structure budgets and contracts to support delivery.** The USCIS CIO spearheaded an innovative contracting approach, which replaced a single large vendor with multiple contractors working together and competing for business. Each contractor provides cross-functional development teams that participate in the iterative product development process, working with federal product owners and project managers. Each vendor is evaluated based on its ability to rapidly deliver working software.

4. **Deploy services in a flexible hosting infrastructure.** USCIS chose to use a "public cloud" infrastructure service provider to host the service. This choice makes it easy and cost-effective for the team to provision, configure and adjust virtual computing resources as needed.

5. **Identify and empower product owners.** USCIS centralized the product development effort in its Office of Transformation Coordination, led by a single executive. This executive has identified product owners for each business line, who are each empowered and responsible for the digitization of that business line's product. Each product owner can prioritize work, advocate for users, and accept delivery of features from the contractor staff. USDS provided training and support to these product owners, and advocated for the creation of this product management structure.

6. **Implement robust monitoring and incident response.** USDS led an initiative to create a rapid response procedure for troubleshooting major incidents such as service outages. This procedure involves identifying "incident commanders" who are empowered to make quick decisions and the use of an alerting tool (currently PagerDuty) to coordinate incident response.

7. **Use "soft launches" to help identify issues prior to full release.** The USCIS team has incremental releases built into its process. For example, the ELIS2 external interface was opened to accept I-90 applications for 72 hours in November 2014. The applications received in this "soft launch" window were then processed using the new system, allowing USCIS to complete an end-to-end test

18-F-1517//1134

of the service with real data. The results of this test were used to refine the service prior to its full launch in February 2015.

8. **Rely on automated tests to increase development speed.** Good automated test coverage allows the team to verifiably demonstrate the system is working as intended, and speeds the development process by providing instant and reliable feedback to developers about how changes they have made to the system have impacted existing functionality. Working together, USDS engineers and contractor teams have increased the use of automated unit and integration tests.

18-F-1517//1135

Streamlining VA Disability Claim Processing

The Challenge

When a veteran has a disease or injury related to service, he or she may file a claim for disability compensation for the service-connected disease or injury. These claims are filed with the Department of Veterans Affairs (VA) and can result in a grant, partial grant, or denial. If a veteran is unsatisfied with the outcome of his or her claim, he or she may file an appeal. Since 1996, the appeal rate has averaged 11 to 12 percent of all claims decisions.

Between FY 2010 and FY 2015, the Veterans Benefits Administration (VBA) completed more than 1 million claims annually, with nearly 1.4 million claims completed in FY 2015. As VA has increased claims decision output over the past 5 years, appeals volume has grown proportionately. Today, there are more than 450,000 pending appeals, and this number is expected to grow to 1 million by 2025 without legislative reform.

The current IT system used to track and process appeals at the Board of Veterans' Appeals and across the VA is more than 20 years old and is built on outdated infrastructure. It powers a variety of workflows essential to the appeals process across VA, but is difficult to use and hard to update, and it is straining under the increased volume of appeals. With such a large volume of paperless cases that travel across jurisdictions within the VA, from the local regional office level to the Board and back again, the VA needed an updated IT solution to ensure full and seamless accountability of all appeals as well as data integrity through integration of systems, increased automation, and reduced manual processes. VA recognized that the processes and technology underpinning the appeals system needed improvements, and began the Appeals Modernization initiative in 2014.

18-F-1517//1136

A screenshot from the current VA IT system used to track and process appeals

Project Impact Summary

- The legacy IT system used to track and process appeals at the Board of Veterans' Appeals is more than 20 years old and is built on an outdated infrastructure.
- A team of three Digital Service at VA staff worked with the VBA beginning in June 2015 to design and implement a new Caseflow Certification tool to provide the Board with all of the information it needs to process an appeal.
- Digital Service at VA developed a script that discovered 2,172 appeals that had been incorrectly categorized and were in limbo. Without this script, appeals in this state may have remained unprocessed for an indefinite period of time.
- As of September 2016, approximately 87.3% of all paperless appeals are now certified using Caseflow Certification. The new tool was successfully rolled out as certification volume increased 34.1% from the year ago period.
- As of September 2016, Caseflow Certification handles 5,000+ certifications per month.

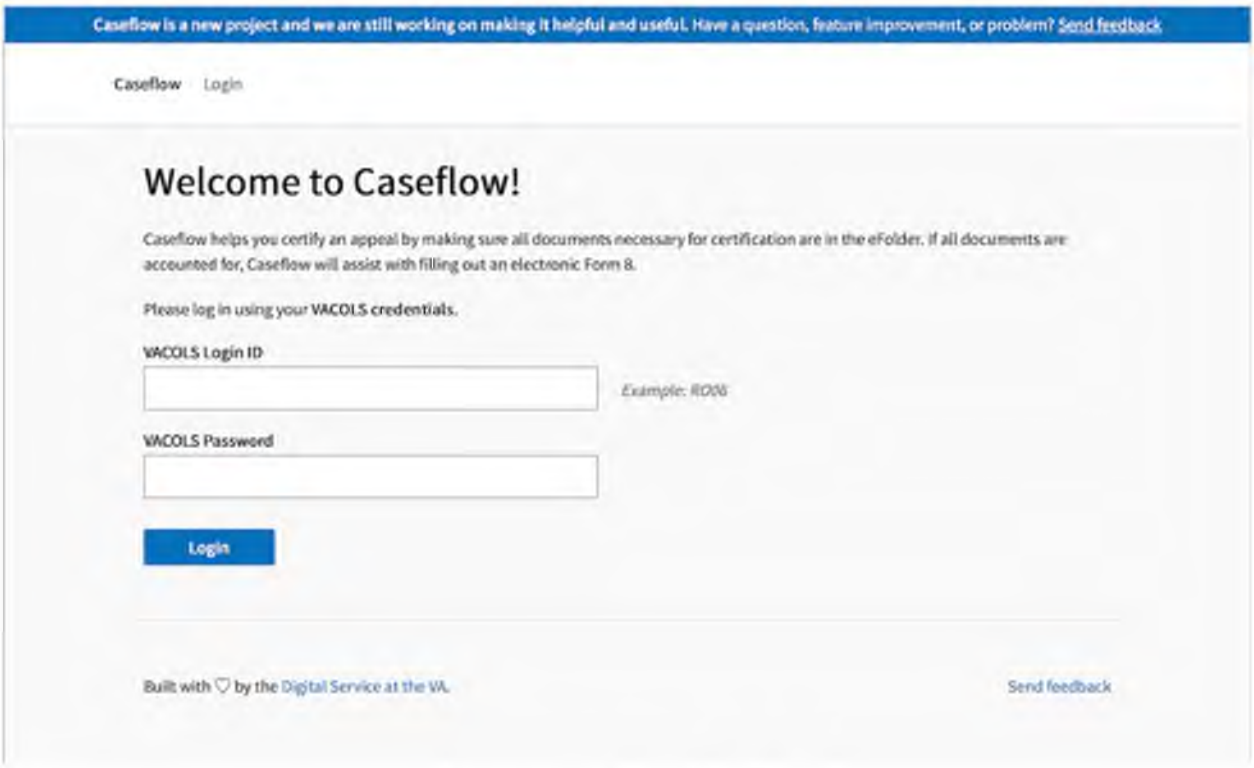
- Digital Service at VA awarded an agile contract on T4NG in September 2016, using a coding exercise to determine contractors' capabilities.
- With a new contract in place, the Caseflow team is growing to 30, including nine Digital Service at VA staff.
- In October 2016, Digital Service at VA began rolling out eFolder Express to the Office of General Counsel and the Records Management Center to improve the efficiency with which appeal documents can be retrieved, including for Privacy Act requests.

The Solution

The U.S. Digital Service at VA (DSVA) – the U.S. Digital Service's first agency digital service team – has worked closely with the Board of Veterans' Appeals to develop a new system that tracks and processes paperless appeals, called Caseflow. This system will have many user-facing web applications that map to existing workflows in the appeals process such as Certification, Activation, Review, and Dispatch. The team is using an iterative approach that will gradually replace small portions of the older system as new components are created, minimizing any disruption to existing business processes. In addition, the USDS modular approach enables quick updates and changes to Caseflow should there be any changes in legislation, regulation, or VA policy.

Caseflow Certification, released nationwide in April 2016, is the first component of the modernized system to be deployed. Caseflow Certification is a tool for VA employees to ensure that the Board has all of the information it needs to process the appeal, and that the data in the claims system — known as the Veterans Benefits Management System (VBMS) — matches the data in the appeals system, known as the Veteran Appeals Control and Locator System (VACOLS). Because many appeals that arrived at the Board contained manual data errors or were incomplete, providing VA employees at regional offices better tools to verify and reconcile key information using automated steps has been critical to optimizing accuracy and efficiency, and ensuring data integrity through system integration. Caseflow Certification also provides a simplified way for staff to generate a VA Form 8 – the Certification of Appeal – which is a required step in the appeal process. The tool automatically populates many fields of this form based on data in the system, reducing manual data entry to just a handful of questions. It also allows staff to file the form in the claims system with a single click, rather than requiring users to switch browser windows, navigate to the veteran's case folder, and manually upload the form.

18-F-1517//1138



A screenshot from Caseflow.

In addition to the user-facing component, Caseflow Certification allowed the DSVA team to develop and run an important script that helps the Board identify pending appeals that may have been incorrectly categorized as paper transfers, when in fact the appeals were paperless. Without this step, the Board could be left waiting for a physical appeal to arrive at its facility when in fact none exists. Without the Caseflow Certification tool, appeals in this state could have remained unprocessed for an indefinite period. The DSVA team discovered 2,172 appeals in this state by running the script. This enabled the VA to proceed with processing these Veterans' appeals, and to take preventative measures to avoid the problem in the future. The DSVA continues to monitor the data to detect appeals that could end up in this state again.

As of September 2016, approximately 87.3% of all paperless appeals are now certified using Caseflow. The remaining appeals are certified using the legacy process, and represent edge case scenarios. The DSVA is working to incrementally improve the Caseflow Certification tool so it can be used in more of these uncommon scenarios. Throughout the rollout, DSVA promptly responded to feedback and issues reported by VA employees.

Success Criteria	Status
All appeals are certified using Caseflow	In progress. At present, 87.3% of paperless appeals are processed using Caseflow.

Milestones

- June 15, 2015: DSVA engagement began
- July-August 2015: Discovery Sprint
- March-April 2016: Caseflow Certification rollout to all VA regional offices
- September 1, 2016: Agile Contract awarded on T4NG with coding exercise
- October 2016: Rolled out eFolder Express to Office of General Counsel and Records Management Center

The Process and Lessons Learned

1. **Understand what people need.** The DSVA team visited the New York Regional Office to collect feedback on Caseflow Certification in October 2015. The team conducted five usability sessions, and used the feedback to improve the tool. The team visited again in December 2015 to gather additional feedback and verify the tool worked as intended in production. Additional usability tests were conducted in the St. Petersburg, Roanoke, Boise and Lincoln regional offices. Testing the service with actual users was critical for building a service that worked for veterans.

2. **Account for training materials and help desk support information.** Prior to rollout, the team needed to prepare training materials for staff who had to use Caseflow. Rather than creating a click-through slide presentation with quizzes, the DSVA decided to record a 5 minute screen share tutorial. Regional Offices provided positive feedback on this format, which they felt was short and specific. In addition to end-user training, the team had to prepare knowledgebase documents for the helpdesk staff who would field support requests from end users.

3. **Launch incrementally.** DSVA established a rollout schedule phased over a month. The team started off with the launch at the New York Regional Office whose employees were most familiar with the tool from the in-person usability

18-F-1517//1140

sessions. From there, DSVA launched in the other regional offices where it conducted remote usability testing. In each subsequent week the team rolled out the application to a larger and larger group of regional offices until it was deployed in all offices.

4. **Ensure application has appropriate monitoring.** The lack of robust application monitoring made it difficult to identify issues with the system. For example, the identity access management service used by the tool went down several times over the rollout period, preventing access to Caseflow. Better monitoring would have allowed the team to identify issues like this before they impacted end users.

5. **Improve automation.** Automation can help improve many aspects of the appeals process (and many similar case processing systems in government). For example, a VA employee shouldn't need to manually re-type information from one system into another system in order to create a form. But there are times in a case processing workflow where human judgment is required. Instead of attempting to account for every edge case, case management systems should automate the most common use-cases, eliminate redundant tasks, and empower staff to use their knowledge and expertise to navigate and resolve tricky edge cases when necessary.

18-F-1517//1141

Simplifying Veteran-facing Services with Vets.gov

The Challenge

Presently, Department of Veterans Affairs' (VA) digital services, such as obtaining a prescription refill, applying for healthcare benefits, checking the status of a claim, and accessing VA forms, are spread across hundreds of public-facing VA websites. Veterans must navigate disparate online systems, remember multiple user names and passwords, and contend with long pages of legalese to access benefits they have earned.

Many of the systems that power these services are outdated and provide a poor user experience. For example, the current digital 10-10EZ form to apply for healthcare was built as a fillable PDF, which requires Adobe Acrobat. The only browser that defaults to Acrobat for PDFs is Internet Explorer, so based on current browser usage, 70% of visitors saw an error message when they tried to apply. As a result, since 2012 only about 8% of all VA healthcare applications were submitted online.

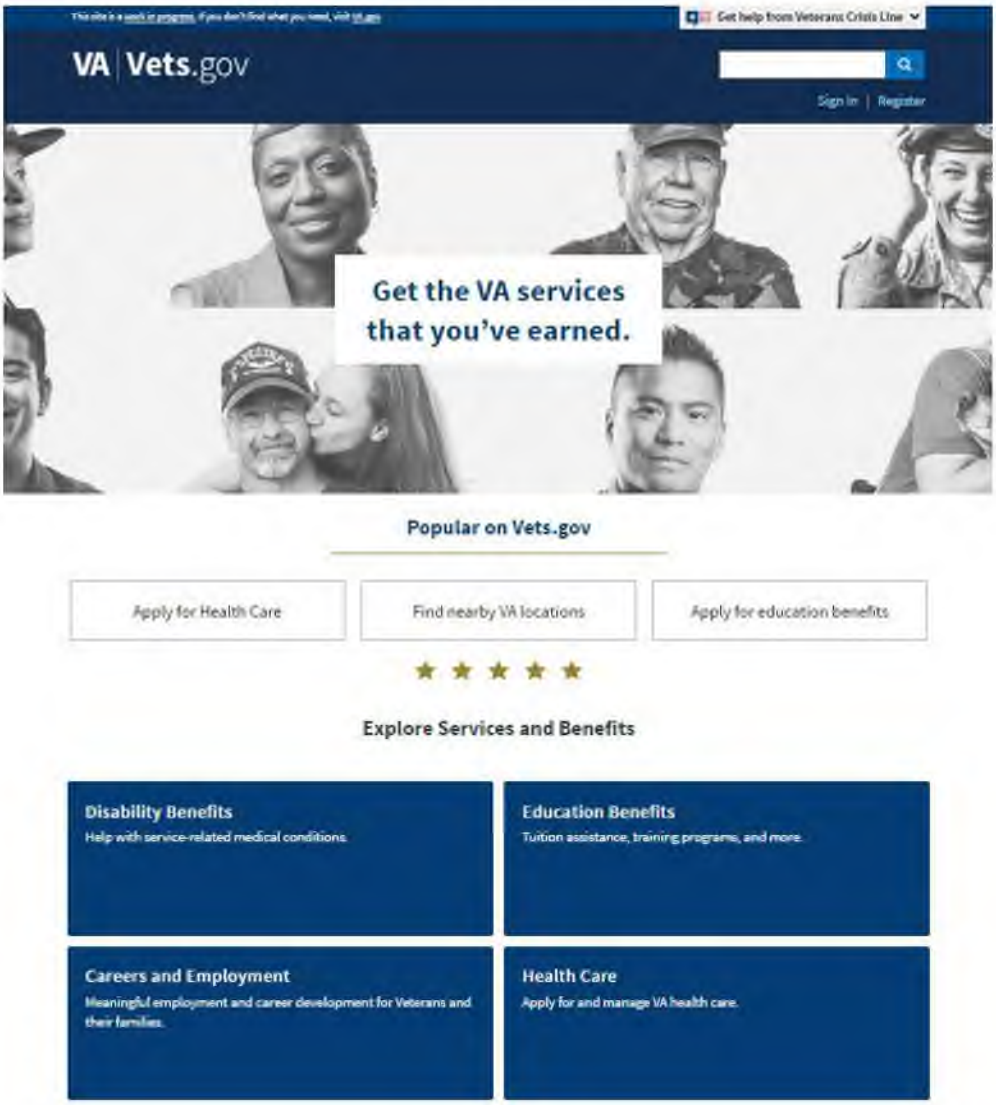
Project Impact Summary

- Many of the systems that power VA's digital services are outdated, and are spread across hundreds of public-facing VA websites.
- In November 2015, the Digital Service at VA launched Vets.gov, a mobile first, cloud-based platform that provides a new way for Veterans to discover, apply for, track, and manage their benefits.
- The initial Vets.gov website included plain language content for education and disability content and several tools: GI Bill Comparison Tool, Facility Location, and a Veteran feedback forum.
- Since then, the vets.gov team has launched 39 products, and reduced release cycle times from 90 days to 7 days.
- In June 2016, a new digital healthcare application was added to Vets.gov. In the first 60 days, 41,000 online submissions were received; an increase from a daily online submission average of 62 per day to more than 500 per day.
- VA is tracking to increase online health care applications from 10% (of 582,000 health care applications received by VA) in 2015 to 50% in 2017.
- In November 2016, the VA Digital Service team will launch several new features including: online application for education benefits, ability to check your disability claim status, prescription refills, secure messaging your health provider, and more.

18-F-1517//1142

The Solution

In November 2015, the VA launched Vets.gov, a new way for Veterans to discover, apply for, track, and manage their benefits. Instead of visiting numerous websites with multiple logins to have their benefits explained to them, Veterans told the USDS design team that they wanted to go to one site to get things done.



The Vets.gov homepage

Specific pieces of functionality planned include the most demanded health and benefits services, such as an accessible health care application that does not require specific software to complete. New functionality will also include claims and appeals statuses, as well as prescription refill services.

18-F-1517//1143

Design and development of vets.gov is led by the U.S. Digital Service at the VA (DSVA) – the first established U.S. Digital Service agency team. It is built with modern, open source tools and is hosted in the commercial cloud. The DSVA is using an iterative development process in which features are continually designed, tested, and integrated into vets.gov. Vets.gov is being built in the open, where Veterans can provide feedback and report bugs directly to the DSVA team, who quickly respond to comments.

Success Criteria	Status
Vets.gov website is available to the public.	Complete. Alpha version launched November 2015. Authority to Operate complete.
Launch digital healthcare application.	Complete. Vets.gov digital healthcare application launched June 2016.
100% of relevant content and front-end functions migrated from 514 existing public-facing VA websites.	In progress. Content related to disability benefits, education benefits, and careers and employment has been migrated to date.
Measurably improved Veteran experience.	In progress. The new online health care application has increased online submissions from 62 per day to more than 500 per day. Metrics collected will include bounce rates, page views, percentage of applications submitted online, volume of support requests to VA call centers.

Milestones

The initial vets.gov website was launched on November 11, 2015. It is a cloud-based platform with a modern technology stack. Immediate benefits and features included the following:

- Mobile-responsive website
- 508 compliance improvements

18-F-1517//1144

- GI Bill Comparison Tool
- Facility Locator
- Disability Benefit content rewritten in plain language
- Education Benefit content rewritten in plain language
- Feedback forum to collect Veteran feedback on the website

Since November, the team has been conducting ongoing research with Veterans and delivered additional content and features on the site, including employment services, the crisis hotline, and most recently the healthcare application.

On June 30, 2016, a new digital healthcare application was added to Vets.gov to enable Veterans to apply for healthcare online, solving the problems that prevented many Veterans from using the previous online application. As a result, the number of Veterans applying for health care online increased from 62 per day to over 500 per day. VA is now on track to increase the percentage of Veterans applying online from 10% in 2015 to over 50% in 2017.

Migration will continue throughout 2016, focusing on the highest demand Veteran services including functionality such as applying for healthcare and obtaining prescription refills.

The Process and Lessons Learned

1. **Understand what people need.** Vets.gov is being designed based on Veteran feedback. The vets.gov team works with Veterans regularly on research activities including usability testing, card sorting, and contextual interviews, using a combination of remote / in-person sessions and individual / group sessions.

2. **Build the service using agile and iterative practices.** Vets.gov is being iteratively developed, with new functionality released incrementally and refined based on feedback from Veterans. To manage this iterative process, the vets.gov team uses industry-standard techniques such as sprint planning and stand-up meetings for each vets.gov product team. These processes enable open communication and fast problem resolution. The whole team holds retrospectives every quarter to review progress and troubleshoot challenges.

3. **Engage stakeholders across the agency.** As a change management tool, the team opened bi-weekly vets.gov 101 briefing to all VA employees and stakeholders. To ensure leadership was fully engaged, the team had regular meetings with the Secretary and Deputy Secretary. The team was fully transparent in its planning and reporting by opening up the vets.gov roadmap to anyone at

18-F-1517//1145

the VA and offering status reports daily to anyone at the VA. Finally, weekly VA Change Management working sessions with communications leads and VA stakeholder meetings helped the team bring diverse players to a common understanding of the vision and goal to ensure success.

18-F-1517//1146

Providing Secure Access to IRS Taxpayer Information

The Challenge

Over 150 million taxpayers interact with the IRS each year. The IRS wants to offer taxpayers digital services such as online access to individual tax records and tax refund statuses. There is clear demand for these services from taxpayers – for example, the "Where's My Refund" online tool is one of the most popular Federal Government websites, with over 200 million requests in 2015. However, providing online taxpayer services is difficult due to the challenge of distinguishing a legitimate taxpayer from an identity thief who may try to steal information held by the IRS to commit fraud. IRS currently withstands more than one million attempts to maliciously access its systems each day.

One important IRS digital service is Get Transcript Online. The tool lets taxpayers access their official tax history, which can be needed for student loan applications, mortgage paperwork, or even filing the current year's returns. In May 2015, widespread unauthorized access of the tool forced IRS to take it offline. After analysis, IRS determined that bad actors had been using taxpayers' personal information stolen from data breaches outside the IRS to circumvent the tool's identity verification process. As a result, some taxpayer information was released to unauthorized users, who used the data to commit tax return fraud.

Creating a new authentication system that solves the difficult challenge of verifying the identity of individuals seeking to use IRS services was a top priority for the agency. Not only would this allow the IRS to restore access to the Get Transcript Online tool, but a method for securely identifying taxpayers is a prerequisite for many future digital services that the IRS is seeking to build for the American people.

One approach considered early in the Secure Access project was to add a "PIN in the mail" step to the user registration process, in which the IRS would mail an activation code to a taxpayer's physical address. The IRS was not satisfied with this solution because it wouldn't provide a better user experience than the default process of simply mailing tax transcripts directly to taxpayers that request them, a process which takes 5-10 days. The IRS wanted a solution that would allow taxpayers to get access to their own data in minutes, not days.

18-F-1517//1147

Project Impact Summary

- In May of 2015, the IRS removed the ability for millions of taxpayers to get online access their tax transcript because the "Get Transcript Online" service had been abused by unauthorized users.
- One option considered to secure the service would be to physically mail transcripts or account PIN numbers. However the IRS wanted a solution that could be completed in minutes, not days.
- A team of three USDS personnel worked with IRS beginning in October 2015 to help design and implement a new Secure Access online process.
- With the help of the USDS team, IRS executed a controlled launch in which the new service was tested with small groups of real users prior to full launch. The team also implemented fine-grained error-tracking and log monitoring. With this approach, USDS helped IRS achieve a 4x reduction in the error rate prior to full launch.
- The new Secure Access process takes an average of 12 minutes for users to complete, compared to the 5-10 calendar day wait for mailed transcripts without Secure Access.
- "Get Transcript Online" was returned to service for all taxpayers using the new Secure Access process in June 2016.
- As of August 22, 2016, taxpayers have accessed over 2.7 million transcripts using the online Secure Access process.
- IRS plans to re-use the Secure Access process for four additional services in IRS' e-Services suite.

The Solution

Recognizing the importance of secure online access, the IRS asked to partner with experts from the USDS in determining how to strengthen their authentication protocols while remaining convenient for taxpayers. Together USDS and IRS outlined the characteristics of a tool called "Secure Access": a user verification process using strong identity proofing and two-factor authentication in line with both industry best practices and federal standards from OMB and NIST.

The new system adheres to the "Level 3" standards of Electronic Authentication Level of Assurance, as defined by NIST in SP 800-63-2. This level of assurance requires an individual to demonstrate control over a physical object (i.e. "something you have") in addition to demonstrating knowledge of personal information such as name, birth date and social security number (i.e. "something you know"). The old system adhered to

18-F-1517//1148

LOA2, which allowed access to the system using personal information as well as knowledge-based multiple choice questions. This level of assurance proved insufficient, because some of the personal information used to verify users' identities in this approach had already been compromised in various data breaches from sources other than the IRS.

Using Secure Access to protect sensitive applications like Get Transcript Online would enable taxpayers to have convenient, real-time access to their transcripts without making that information vulnerable to automated fraudulent attacks. Working side by side with the agency, USDS helped IRS deliver the Secure Access project following principles from the Digital Services Playbook. These proven approaches enabled the IRS to efficiently deliver the Secure Access project in a timely manner. In June of 2016, the IRS launched Secure Access and brought Get Transcript Online back into service.

Success Criteria	Status
Restore online access to tax records in a manner that is secure against automated attacks (implementation of the NIST Level of Assurance Level 3 standard)	Complete. Service launched in June 2016. As of August 22, 2016 taxpayers have accessed over 2.7 million transcripts.
Build an account creation process that takes less than 15 minutes for a user to complete.	Complete. Account creation takes an average of 12 minutes, vs. 5-10 days for mailed transcripts or PIN numbers.
Implement error tracking and log monitoring. Collect and report daily business metrics.	Complete. Daily statistics on attempts, pass rates, error rates and overall traffic are collected and disseminated. Error tracking and log monitoring implemented. Phased launch strategy resulted in fourfold reduction in error rate.
Secure Access process used for at least one additional IRS service in addition to Get Transcript Online.	Complete. Secure Access is now used for the "Get an Identity Protection PIN" service in addition to Get Transcript Online. IRS also plans to implement Secure Access for four additional services in IRS' e-Services suite (Registration Services, e-File Application, Transcript Delivery, and TIN Matching).

18-F-1517//1149

Milestones

- October 2015: Discovery Sprint completed
- November 2015: Project start date
- February 2016: Secure Access protocol code completed
- March 2016: Internal employee test
- May 2016: Service launched to production, beginning controlled phase-in approach
- June 2016: Service launched to all users

The Process and Lessons Learned

1. **Assign one leader.** The IRS recognized the need for a single executive to help provide consistent oversight over all authentication and authorization needs across the many IRS functions and channels. They created the Identity Assurance Office, led by a senior IRS executive with experience working with both business and information technology groups. USDS worked side by side with this executive, helping clarify the business, product, process, and technical decisions that come with the responsibility of meeting user demands. USDS also worked with partners at OMB and NIST to get relevant background information that would help this leader make decisions that would meet federal standards while also meeting both user and business needs.

2. **Understand what people need and design a simple and intuitive service.** USDS worked with the IRS team to maintain constant focus on taxpayer needs. At the beginning of the project, USDS gathered input from the United Kingdom's Government Digital Service to inform early directions and learn from this organization's hard-won experience. One of the key insights from the U.K. team proved particularly valuable. The U.K. team learned it was important to set user expectations about how the authentication process would work up front, and to provide graceful alternatives if the user cannot or does not wish to continue with the online authentication process.

   USDS worked with the IRS to create draft user flows and tested them with users on a weekly basis. USDS improved the navigation, flow and messaging based on these tests. For example, an early prototype confused taxpayers by stating that authentication would require a "Credit card or auto loan, mortgage, home equity loan account number." In usability tests, the team learned that taxpayers thought they needed the account number for the credit card, not just the last eight digits of the credit card itself. The team changed the wording to be clearer. The IRS will

18-F-1517//1150

continue to use this iterative design process to help determine which features and fixes should be prioritized.

3. **Build the service using agile and iterative practices.** In addition to the iterative design process described above, at the suggestion of the USDS, the IRS used a phased launch process to test and refine the Secure Access protocol before its full launch. Initially, the agency limited access to the authentication system to only IRS employees. This controlled test allowed the team to get end-to-end user data that accelerated debugging and improvements.

4. **The USDS worked together with developers and business analysts to understand how users were getting stuck in order to improve the process.** An example of an issue that was discovered and fixed in this controlled launch was in a data entry field. When users were prompted to enter their account number, some users included the "#" character when typing the number. This would generate an error message that explained the "input was too long," confusing users. This problem did not surface in internal quality assurance testing, and would not have been discovered without letting real users interact with the system prior to full launch. The team fixed the problem and redeployed the improved code to another cohort of internal users. After this internal test, the IRS used a public beta period where the improved Get Transcript Online service was offered to a small percentage of public visitors to the IRS website. This beta period allowed the team to fix even more issues. This iterative process was used to identify and fix many subtle errors and points of confusion prior to full launch.

5. **Use data to drive decisions.** Collecting good data on how users were interacting with the system was a key to success. With USDS assistance, the IRS developers implemented fine-grained error codes and log monitoring. With this data, the team could categorize bugs and list the most common errors, allowing the team to prioritize its efforts. In one such case, a bug that resulted in a small number of users in the public beta test being unable to register was identified and eliminated. In this case, USDS engineers examined the code and speculated that an input validation filter on one of the field items had been accidentally set too strictly, rejecting some valid inputs. An IRS developer used the error monitoring data to identify that the error was highly correlated with specific versions of the Firefox web browser. With these insights, the team was able to identify the root cause of the error and deploy a fix before the tool's public announcement, saving hundreds of users a day from having the same issue.

   Between the initial deployment of the Secure Access protocol and the full public launch, iterative development coupled with good monitoring allowed the IRS to

18-F-1517//1151

achieve a fourfold drop in the error rate. The agency will continue to monitor errors and prioritize effort based on this data.

18-F-1517//1152

Improving the Visa Processing System at Department of State

The Challenge

The Department of State (State) protects the lives and interests of U.S. citizens overseas and strengthens the security of U.S. borders through the vigilant adjudication of visa and passport applications. State provides a range of services to U.S. citizens and foreign nationals, including issuance of U.S. passports and Consular Reports of Birth and Death Abroad and adjudication of nonimmigrant and immigrant visa applications. These processes largely are conducted through a collection of custom applications that depend on a system called the Consular Consolidated Database (CCD).

Many government systems, including the CCD, were designed at a time before most modern technologies to support distributed data processing were available. As a result, CCD's technical approach – innovative at the time it was implemented – deviates from what are now industry best practices. Over time, development focused on adding new features rather than modifying the underlying platforms and tools.

The integration of various components made the CCD progressively more complex. As a result, it became more difficult to ensure new features were integrated in a high-quality, easily maintainable manner. As demand increased, some tools were not able to be improved upon in a timely fashion.

Project Impact Summary

- In June 2016, the USDS team began discovery work around how to improve the visa application process. The team honed in on better ways to update applicants and petitioners on case status by making adjustments to a tool built in 2012.
- Over the past year, the CEAC Visa Status Check site received over 3 million visits per month from users ranging from petitioners in the United States to applicants across the world.
- The National Visa Center, a visa application processing center run by the Department of State, receives approximately 9,000 phone calls a day. The vast majority of those calls are about a visa applicant's case status.
- The USDS team, in partnership with the Bureau of Consular Affairs, is in the process of engineering improvements to the tool that will show users better

18-F-1517//1153

information about their case status and how to advance to the next stage of the application process.

- The USDS team performed robust user testing of the new status tool and tested how improved information using plain language may help cases move more quickly through the appropriate parts of the process.
- The status tool will launch soon. We will measure the impact of the tool against several metrics, including how it impacts the National Visa Center's call volume.

The Solution

USDS worked closely with State's Bureau of Consular Affairs' Office of Consular Systems and Technology (CST), which supports, develops, and maintains the technology that enables a global network of consular systems to support U.S. consulates and embassies, domestic visa processing centers, and domestic passport processing agencies and centers. CST already had a number of viable plans to improve overarching stability of the CCD and related applications, but attempts to execute these plans had been stymied by the system's complexity. USDS served as technical consultants, both vetting possible solutions and advising on industry best practices and as an empowering authority facilitating communication across divisions and organizations.

Success Criteria	Status
Standardize software development processes and tooling, enabling the Federal Government to have better visibility into contractor-developed custom software.	Completed. Established central source control repositories on a unified source control system. Completed a pilot that has improved developer workflows and allowed greater oversight into how code is being developed.
Transition how information is batched and sent to partner agencies to ensure there are no artificially created backlogs.	Completed. Changes made from both ends have been implemented and information is more efficiently transferred between agencies.
Immigration process and status is clear and comprehensible to applicants.	Ongoing. USDS team is currently implementing improvements to an existing tool that should more clearly communicate case status to applicants.

18-F-1517//1154

Milestones

- December 2015: USDS began engagement to improve information security of various State applications.
- February 2016: USDS began exploration of what kind of developer tools were needed within State to improve engineering practices.
- March 2016: State received USDS recommendations for improved developer tools, including usage of version control software.
- April 2016: USDS began assisting a State vendor with implementation of a version control software pilot.
- April 2016: USDS began discovery work on how to improve how State transmits information for Security Advisory Opinions with partner agencies.
- June 2016: USDS began determining ways to improve how visa status information is shared with applicants, petitioners, and their agents.
- June 2016: Technical implementation of the Security Advisory Opinion data sharing process began.
- July 2016: Technical implementation of improvements to visa status check tool began.
- September 2016: Completion of the technical and business process changes for the Security Advisory Opinion data sharing process.
- September 2016: USDS completed work on a pilot that saw a number of contractors using modern software development tools in the form of version control software.

The Process and Lessons Learned

1. **Working with and Empowering the Agency:** State identified a number of areas where it could improve its information security. USDS provided assistance in the form of consultation on system remediation and coordination of implementation. USDS also worked closely with teams within State to identify how to prioritize various kinds of remediation that needed to be implemented and how to rank ongoing concerns. Using these techniques, State has markedly improved its defensive posture.

2. **Breaking Agency Silos to Solve Problems Together:** In many cases both the technical expertise and the most appropriate solution were already present within the organization. However, in an agency the size of State it is sometimes difficult to convene these groups and share solutions to senior leadership and across the agency. USDS conducted extensive site visits to bring various branches and contractor groups across State together, and with State leadership's help was able to create cross-team collaboration that sped up the development and deployment of solutions. The project to modernize developers' tools, for

18-F-1517//1155

example, is a collaboration between multiple divisions within CA/CST: Configuration Control, Systems Engineering and Integration, and Service, Systems and Operations.

3. **Technical Vetting and Evaluation:** USDS provided State program and project managers with objective technical advice. This gave State better accountability and communication among contractors. Since problems were often spread over applications and systems governed by several contracts, government managers heard different technical explanations. USDS engaged in several "fact finding missions," allowing State to use this information to prioritize tasks effectively.

4. **Embrace pilots:** Pilots are great opportunities to perform experiments in a contained, structured way. The ability to experiment is essential when bringing on new tools, services, or methodologies. It's not clear which will work best in a given environment, so experimentation is essential to bringing new tools, services, and methodologies to an organization. Knowing that the results will be used to determine if a pilot will continue helps stakeholders embrace new methods of doing things.

5. **Test early and often:** Manual and automated testing are essential parts of the software development process. Increasing your test coverage makes it easier to deploy a tool or functionality quickly and securely. We are hopeful that by working with stakeholders and contractor teams, we can improve the testing culture for how Department software is developed.

18-F-1517//1156

Helping CMS Implement Congressionally Mandated Medicare Payment Changes

The Challenge

In April 2015, Congress passed the Medicare Access & CHIP Reauthorization Act of 2015 (MACRA), changing the way Medicare pays doctors for services rendered to patients enrolled in the Medicare program. The act implements changes designed to reward health care providers for giving better care, not just more care. These changes will impact a large percentage of Medicare Part B payments, and the Centers for Medicare & Medicaid Services (CMS) seeks to ensure the transition from the current payment program to the new system is simple, clear, and effective.

Project Impact Summary

- Implementation of the Medicare Access and Chip Reauthorization Act of 2015 required a transition of payment programs that would impact a large percentage of Medicare payments to doctors.
- CMS engaged the USDS team to draw on best practices from other large program implementations.
- CMS created an integrated project team that combines policy and operations, and uses agile methodologies and other modern technology practices.
- The development team has employed user research, user need analysis and constant iterative feedback loops with users to ensure transition success.
- On October 14, USDS helped CMS released the Final Rule for implementing MACRA concurrently with a plain language website describing the rule. The website serves two purposes: first, to help clinicians and their partners easily understand how MACRA impacts them and, second, to serve as a single entry point for clinician interaction with the program in the future.
- The MACRA implementation is still on-going and iterative development will continue throughout 2017.

The Solution

MACRA implementation is an important priority at CMS. USDS is helping CMS take an implementation approach that draws best practices learned from implementing other large programs, including HealthCare.gov and the adoption of the 10th revision of the

18-F-1517//1157

International Statistical Classification of Diseases and Related Health Problems (ICD-10) standard. Key priorities include widespread user research and user needs analysis, an integrated project team across CMS responsible for program delivery from policy to operations, a tight iterative feedback loop with users to inform program design and ensure that it is clear and accessible, and incorporation of modern technology best practices.

Success Criteria	Status
Contracts for key elements of MACRA implementation are agile and responsive to evolving program needs.	In progress. CMS has successfully used agile acquisition practices across most of the contracts for the MACRA program.
Project team is integrated and running off of a shared roadmap for execution, including user research, policy, procurement, operations, technology, and analytics.	In progress. CMS has identified a product owner for MACRA implementation. CMS staff and contractors work on an integrated team.
Modern technology development best practices are being used in the creation of program infrastructure.	In progress. USDS assisting CMS staff and contractors to implement best practices in design and engineering.

Milestones

- February 2016: USDS Discovery Sprint/Project Started
- May 2016: Development work started
- October 2016: Final Rule with Comment and website concurrently launched

The Process and Lessons Learned

1. **Go where the work is.** The USDS team has pushed for extensive collaboration and information sharing between the USDS, CMS, and its contractor teams. The USDS team works alongside CMS staff and contractors on an integrated team at least four days a week in a shared space to facilitate this goal.

18-F-1517//1158

2. **Engage agency leaders and policymakers in the process.** The USDS team works hand-in-hand with CMS leadership on the program. The team is helping to ensure that implementation details, technical trade-offs, and operational complexity are communicated effectively to the whole team, including those writing policy.

3. **Identify a product owner.** CMS identified a single product owner for the implementation of the law, which has facilitated faster decision making.

4. **Provide contracting officers with agile acquisition training.** The CMS team was aware of agile acquisition practices, and their ability to implement agile contracts was significantly helped because one CMS contracting officer had already gone through the USDS agile acquisition training program. CMS has successfully utilized agile acquisition practices across most of the contracts for the MACRA program. The head of the division has further requested more training in agile contracting for the entire team.

18-F-1517//1159

Reducing Inefficiency in the Refugee Admission Process

The Challenge

In Fiscal Year 2016, President Obama set a ceiling of admitting 85,000 refugees into the United States. This represented a 15,000 person increase over the previous fiscal year's ceiling, and this increase depended upon improving the efficiency of the refugee admissions process.

One of the most impactful improvements was the introduction of the digital approval process for refugee applications. Previously, Department of Homeland Security (DHS) officers were only able to approve refugee registration forms using an ink approval stamp in the field where the refugee file is physically located. 57% of cases are finalized on a different day than the DHS field interview. In many of these cases the requirement for an ink approval stamp added an unnecessary delay of up to eight weeks after all security checks had been completed, as cases waited for a DHS officer to travel back to the field location where the file was located to stamp it approved.

Project Impact Summary

- In December 2015, USDS, the State Department, and the Department of Homeland Security established an interagency Refugee Coordination Center (RCC) staffed with representatives from each agency.
- The RCC began working on a prototype for digital approval of cases in January 2016 and launched the product for DHS use in June 2016.
- By September 30, 2016, 11,571 individuals had been digitally-approved, helping the Administration meet its refugee admissions goals while maintaining integrity in the process. Furthermore, the digital approval process codified rigorous security standards, granted DHS flexibility of when and where it can spend time doing administrative work, and saved the Department of State's Resettlement Support Centers time and money by eliminating the need to prepare and ship case files for ink approval stamping.
- State Department Resettlement Support Centers (RSCs) processing these cases stated that the following amounts of time were reduced in the admissions process as a result of the launch of the digital approval process: Bangkok: 1-2 months; Malaysia: 1-2 months; Middle East and North Africa: 1-6 weeks; South Asia: 15 days; Latin America: 15 days; Africa: 12 days.

18-F-1517//1160

The Solution

The digital approval process enables DHS officers to digitally-approve a refugee registration form without having to physically travel to apply an ink stamp on paper. The solution was created by granting DHS editing rights to the State Department's refugee case management system for the first time. Filters ensure that only cases ready to be approved appear for DHS to digitally approve.

In order to convert the manual process into a digital process, the RCC worked with DHS officers to convert all of the manual steps to approve a case into the new digital approval feature. These included:

Checking security statuses

In the manual process, DHS officers are required to physically review a security report for each individual on a case and annotate the page attesting that they have reviewed each page. In this digital approval process, DHS officers electronically affirm they have reviewed all security statuses and the case file, which then enables them to click the digital approval button.

Updating the hard copy form

In the manual process, DHS officers have a paper form that is a history of all actions made on a case. In the digital process, once a digital stamp is applied, the system automatically generates a new digital file for the case, including the time and date the case was digitally-approved, and is included in the case's physical file by the State Department.

Approving the I-590

In the manual process, DHS officers physically approve a refugee registration form (Form I-590) by applying an ink stamp to the approval block on the form. In the digital process, DHS officers click "stamped approved" and the system securely and automatically-generates an individual-level approval page with the time stamp and name of the approving DHS officer. The RSC staples this file to the front of the refugee form, which Customs and Border Protection reviews upon the refugee's arrival at a port of entry in the United States.

Approval Letter

In the manual process, once a case is ready for approval DHS officers initial an approval letter. State Department Resettlement Support Centers then date the letter before

18-F-1517//1161

scanning it and then delivering to the refugee. In the digital process, the system automatically-generates an approval letter with the approving officer's initials and the time stamp when the case was approved, and it is automatically-saved in the case's digital file. The Resettlement Support Centers print and deliver the approval letters to the refugee.

The Role of the RCC

In addition to these process modernizations, USDS assisted with data modeling to predict the number of people who would benefit from digital approvals in order to justify dedicating engineers' time to develop this feature. USDS also designed the system requirements, created prototypes, and coordinated agency-wide approvals for the project. USDS then worked with State Department engineers to develop the new features, and with DHS officers to test the features prior to launch. USDS assisted with the phased roll-out of the digital feature, including training of DHS officers and development of Standard Operating Procedures (SOPs). Finally, USDS ensured that USCIS notified all stakeholders within DHS to prepare components for these changes prior to the first digitally-approved cases arriving in the United States.

Success Criteria	Status
Reduce the time between the date a case is ready for approval and the date it is approved to under two weeks.	On track. In August 2016, of all cases that were digitally-approved, 74% were approved in five days or less and 56% in two days or less. Of the 124 cases that took more than 15 days to digitally approve, 77% did not need to travel until January 2017 or later.
Reach 8,000 individuals approved digitally before the end of the fiscal year.	Complete. 11,571 individuals were digitally-approved by the end of the fiscal year.
Ensure at least 20 officers were part of the digital approval pilot.	Complete. By the end of the pilot, more than 60 officers were trained and had permission to use the digital approval process.

Milestones

- January 2016: Began prototyping and requirements gathering for the digital stamp

18-F-1517//1162

- March 2016: Finalized all data analysis, cost benefit analysis, completed requirements
- May and June 2016: State Department engineering team developed digital approval feature
- June 2016: Conducted user testing and fixed bugs in the system
- June 2016: Digital approval process launched
- September 30: Digital approval process pilot ends and full roll-out began

The Process and Lessons Learned

1. **Engage stakeholders across the agency and collaborate with subject matter experts.** Engaging stakeholders across the agency and working with civil servants who are subject matter experts was essential for the success of this project. In this case, the concept of digitally processing cases had previously been identified by individuals at DHS as an opportunity to increase efficiency. Identifying and collaborating with these individuals allowed USDS to make progress faster.

2. **Keep the scope narrow for the minimally viable product (MVP).** Despite pressure to expand the scope of the MVP that was prototyped, development remained focused on the most critical features for refugee officers and refugees. Throughout the development process, USDS focused on core user needs, replicating the existing physical process into a digital experience. This narrow focus ensured that work flows would remain largely unchanged for refugee officers.

3. **Understand users' needs by testing with actual users.** The digital approval process was built with input from internal users to ensure their feedback was understood and addressed prior to launch. While quality assurance testing by Department of State engineers was critical, USDS' time spent with DHS end users was important for uncovering a variety of issues that would not have been found through engineering team testing alone.

4. **Rely on pilots and build up to a successful launch.** USDS relied on an initial pilot period (from June 24th through September 30th) with limited users (at first only one user and by the end more than 60) to identify any new glitches. Additionally, USDS worked with DHS to develop Standard Operating Procedures and video, teleconference, and in-person trainings to ensure ease of use and clear understanding of the new digital process. Once the digital approval process was judged to be successful and stable with the small pilot group, it was rolled

18-F-1517//1163

out more broadly to additional users. There was unanimous support to roll out the digital approval process to all trained and eligible users in Fiscal Year 2017.

18-F-1517//1164

Helping Students Make More Informed College Choices at Department of Education

The Challenge

For students, higher education may be the single most important investment they can make in their futures to ensure they have the knowledge and skills needed to compete in an increasingly global marketplace. College is the surest path to becoming part of America's middle class and for this reason, selecting a college is an incredibly important decision for many people. But, many potential college students and their families do not have the advisors or resources to help them find a college that will serve them well.

With college costs and student debt on the rise, the choices that American families make when searching for and selecting a college have never been more important. Yet, students and the organizations that serve them struggle to find clear, reliable, and comparable data on critical questions of college affordability and value, such as whether they are likely to graduate, find middle-class jobs, and repay their loans. At a time when America needs colleges to focus on ensuring affordability and supporting all students who enroll, many of the existing college rankings instead reward schools for spending more money and rejecting more students. Additionally, college leaders and state policymakers who seek to improve institutions' performance often lack reliable ways to determine how well their schools are serving students.

To address this challenge, the Department of Education sought to redesign the College Scorecard.

Project Impact Summary

- The USDS team at the Department of Education, with help from 18F, launched the College Scorecard to help students and their families make more informed choices about where to go to school.
- The Scorecard makes comprehensive data on college costs, graduation rates, graduate debt, repayment rates, and post-college earnings accessible to help students choose a school based on access, affordability and outcomes.
- The project drew on hundreds of interviews with students, parents and guidance counselors to ensure that the product would fit their needs.

18-F-1517//1165

- In its first two weeks, College Scorecard attracted over 850,000 unique users, a major uptick from the 160,000 who used the prior version of the tool the entire year before.
- The project opened the data to the public and made an API available specifically for third-party developers to build more applications to help students and policymakers. More than a dozen organizations have built new tools using this data.
- Google has now integrated College Scorecard data so that it shows up front and center in the results of hundreds of millions of education-related searches.

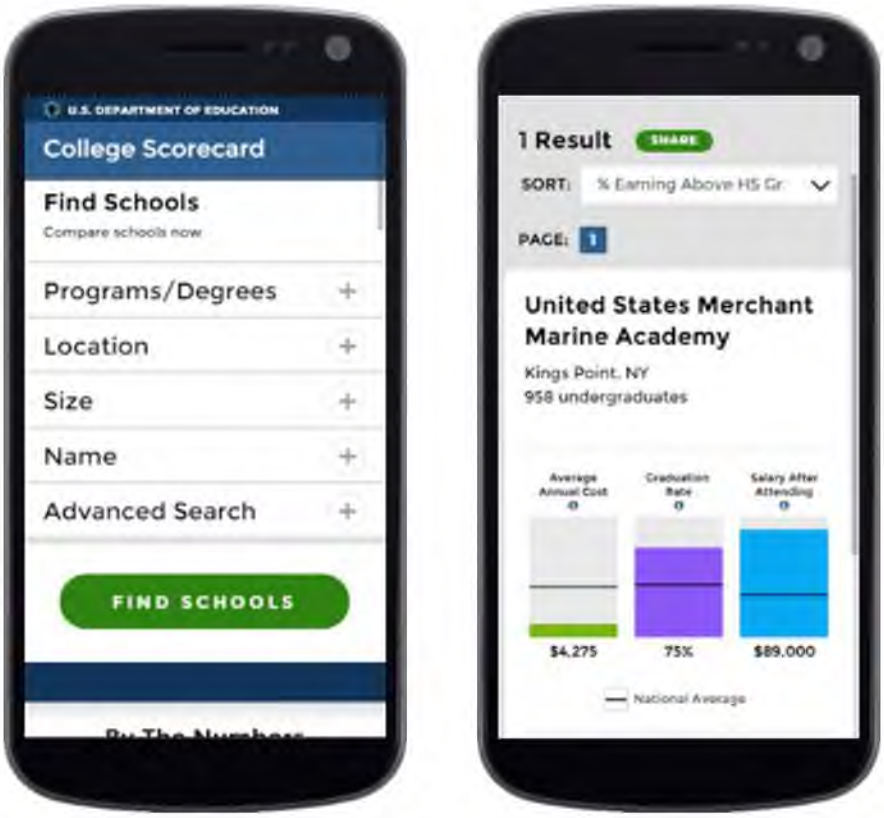
The Solution

The new College Scorecard was redesigned with direct input from students, families, and their advisers to provide the clearest, most accessible, and most reliable national data on college costs, graduation rates, and post-college earnings. This new College Scorecard can empower Americans to rate colleges based on what matters most to them; enable policymakers and the public to highlight colleges that are serving students of all backgrounds well; and focus greater attention on making a quality, affordable education within reach. The new tool for assessing college choices, with the help of technology and open data, makes it possible for anyone—a student, a school, a policymaker, or a researcher—to evaluate an institution on the factors that matter most to them.

The public can now access the most reliable and comprehensive data on students' outcomes at specific colleges, including former students' earnings, graduates' student debt, and borrowers' repayment rates. This data is published through an open application programming interface (API), enabling researchers, policymakers, and developers to customize their own analyses of college performance more quickly and easily.

More than a dozen organizations are using this data to build new tools. For example, Scholar Match, Propublica, and College Abacus—three college search resources—are using the new, unique data to help students search for, compare, and develop a list of colleges based on the outcomes data that the Department of Education made available for the first time through an API. InsideTrack, comprised of a team of coaches and consultants working to improve student outcomes by helping students find the institutions that are right for them, uses the data to develop and implement effective student-centered initiatives.

18-F-1517//1166



The College Scorecard

The Department of Education plans to continue releasing new College Scorecard data and promoting use of these new access, affordability and outcome metrics.

Success Criteria

Success Criteria	Status
Engage a diverse set of students and their supporters, especially high-need, low-income and first-generation college-goers.	Ongoing. In the first two weeks the Scorecard was launched, it was accessed by 850,000 users. The previous version of the tool received 160,000 total users in the previous year.
Educate the marketplace and shift focus to key outcome metrics and institutional performance	Ongoing. External organizations and third party developers are making use of this new data in their tools and research.

18-F-1517//1167

Success Criteria	Status
Enable more informed college matching	Ongoing. As of September 2016, 1.5 million unique users have accessed the tool. The previous version of the tool received 160,000 unique views a year.
Foster continuous improvement	Ongoing. New data was released to the Scorecard in September 2016. All Scorecard information is now appears in search results for colleges.

Milestones

- April 2015: Project Start Date.
- July 2015: Code Start Date.
- September 2015: Go-Live Date.
- May 2016: USDS Project End Date.
- September 2016: New data released to Scorecard. All data indexed and searchable.

The Process and Lessons Learned

- **Understand what people need.** USDS, Ed, and 18F built College Scorecard by working with users at every stage of the project to find out how they made decisions about college. The team met with students (both high school and adult), parents, guidance counselors and advisors, open data users, and people who wrote to the President about their college search experiences. Long before the first line of software code was written, the team was working with students, testing paper prototypes to make sure they were as easy-to-use as possible.

18-F-1517//1168

Getting feedback on a paper prototype of the new College Scorecard.

- **Build services using agile and iterative processes.** The Department of Education built the College Scorecard using agile development methodology. To deliver the right product — what students actually need — as efficiently as possible, the team built the new College Scorecard using an approach that allowed the team to work in short iterations, and to test, scale, and design the tool with a process that could adapt to changes in technology and user needs. The team maintained a project rhythm of two week iterations, with daily stand up meetings to coordinate progress.

- **Run a developer beta.** USDS ran a beta specifically for developers — giving them a chance to test the data and documentation and flag opportunities to make it even easier to use. The feedback from the developers made it possible to release the data in a way that led to easy re-use by third parties.

- **Launch a minimum viable product (MVP).** The team focused on launching a MVP, building the right products to meet customer needs as efficiently as possible. This approach allowed the project to launch with less than 3 months of development time. The team built the project mobile-first and focused on the most critical feature set and information that each user type advocated for.

- **Release open data, and build services using the same APIs offered to the public.** Rather than focusing solely on creating a user-facing website, the team

18-F-1517//1169

also created documentation for, and released, open data for over 7,300 colleges and universities, going back 18 years. This made it possible for third-parties to incorporate the data into their own products and tools, increasing the chance that the information makes it to users wherever and whenever they might be looking for it.

To make it easier for third parties to integrate this data, Department of Education published an API. This API serves both as the engine for the College Scorecard itself as well as a source for external software developers or researchers who want to use the data in their own digital products. The College Scorecard effort is one of the first government digital services that not only releases open data, but also builds a user-facing tool on top of the very same API it provides to the public. This is a common practice used by American's best technology companies.

18-F-1517//1170

Modernizing the Department of Defense Travel System

The Challenge

The Defense Travel System (DTS) provides travel for all Department of Defense (DoD) employees (excluding permanent changes of station). While the DTS does provide end-to-end travel and expense functionality, the antiquated system provides a poor user experience and limited reporting capability. The system has long been a pain point for DoD travelers and officials, and has been scrutinized by lawmakers and auditors. For example, after the Government Accountability Office determined that DoD had overestimated savings for DTS and failed to fix implementation problems with the system nearly a decade ago, DTS added fees for the user and prevented travelers from quickly making changes to their reservations. Lawmakers have required the DoD to improve Defense travel through the creation of the Defense Travel Management Office (DTMO) and providing them with the Defense Travel Pilot Authority to find ways to improve the system and agreements that govern Defense travel.

Currently, the Department of Defense's travel spend is over $8.7 billion per year. Of this spend, $3.5 billion is handled through the DTS, with a per-transaction cost around $10. In addition, there are over 1600 pages of DoD travel regulations. Despite this, about 100,000 unique users access DTS daily, according to the DoD website.

The complexity of the Joint Travel Regulations imposes a challenge for standard DoD users, as well as Authorizing Officials who administer and authorize travel. Many of the policies make it difficult to apply commercial best practices to the system. For example, the policy precludes the integration of industry-standard features like restricted fares, which could ultimately lead to higher cost savings across the department.

Project Impact Summary

- The Department of Defense has long needed to improve the costly and cumbersome system used to book, expense, and manage travel for its employees.
- In March 2015, the Digital Service team at the DoD started working with agency staff to identify a new, commercial tool to better manage travel, and agreed to oversee a pilot test of the new system.
- At the same time, DoD worked to simplify its complex travel policy, with an eye toward saving millions of dollars and delivering a better user experience.

18-F-1517//1171

- In June 2016, the new software-as-a-service travel tool and streamlined policy were in place, and a pilot opened for "basic travelers." Both are still being refined.
- This project demonstrates the potential of pairing policy development with technology implementation to produce more efficient outcomes, and reinforces the principle that using commercial software when minimal customization is required can save the Federal Government significant time and money.

The Solution

To reduce costs and improve the customer experience, DoD is seeking to modernize its travel system with a commercial software-as-a-service (SaaS) product. At the same time, DoD has committed to simplifying the travel policy under the Joint Travel Regulation (JTR). These changes have the potential to save hundreds of millions of dollars per year and improve satisfaction of Defense travel customers. The Deputy Secretary of Defense has directed the relevant human resources and travel offices to complete the policy review and the initial technical transition. The USDS' Defense Digital Service team assisted DoD and its DTS contractor in identifying a commercial vendor that could meet its requirements without requiring expensive customization.

The Defense Digital Service team is also helping DoD pilot this new system. The pilot, now underway, is focused initially on a small population of "basic travelers" using a streamlined travel policy subset. Over time, the project will scale in size and complexity. Concurrently, an effort is underway to considerably simplify the JTR by consolidating the types of travelers.

Success Criteria	Status
New DTS tool released	In progress. Tool has been identified, and is currently being piloted.
Policies governing DoD travel simplified	In progress. An effort is underway to considerably simplify the JTR by consolidating the types of travelers.
Increasing DTS customer satisfaction rating	In progress. As of June 2016, pilot is underway.

18-F-1517//1172

Success Criteria	Status
All travel request processed in new DTS system	Incomplete. Small pilot underway.
Improve data collection to enable better market position with travel vendors	Incomplete. Underway.

Milestones

- March 2015: DTS Sprint begins.
- June 2016: First user booked travel in the new system.

The Process and Lessons Learned

1. **Digital services are only as good as their underlying policy.** Many of the challenges with the current DTS system stem from the complexity of the Joint Travel Regulations. Without updates to this policy, it will be difficult to modernize the DTS. For example, the Joint Travel Regulations require pre-obligation, which is the act of obligating funds for travel prior to the trip based on the trip's estimated cost. This pre-obligation estimate is intended to prevent a trip from costing more money than is available, and includes transportation, hotel, per diem, and incidentals. However, many standard commercial travel solutions cannot easily accommodate pre-obligation estimates, so the DoD is working to change the current policy requirements to avoid requiring system customization. One solution being proposed is to estimate total travel costs and make a budgetary hold on the funds so that approving official will not approve trips in excess of an approved budget. Another potential solution also includes making an estimated bulk obligation based on historical expenditures.

2. **Test services with users as early as possible.** While the new system is being developed for use by all users, DoD is piloting it with certain types of travelers who have basic requests. DoD is following an industry best practice of launching systems earlier in their development, even when not all aspects may be fully automated. This will enable the team to improve the system based on real-world usage information.

18-F-1517//1173

3. **Use commercial cloud software services when possible, but be wary of commercial solutions that require extensive customization.** The modernized Defense travel system is being delivered using a commercial software-as-a-service travel tool, allowing DoD to avoid an unnecessary custom software development project. This is a best practice to follow when the commercial solutions require minimal customization to meet the government's needs. The DoD is seeking to avoid custom configuration requests for this service as much as possible, understanding that the expense and difficulty of such customizations often negate the benefits of using commercial services, and can lead to vendor lock-in.

4. **Modernization efforts should have clearly defined objectives.** If the success criteria above are met, this will enable the DOD to achieve the three main goals of modernizing the DTS: 1) Provide users a better customer experience, 2) increase the volume of trips, travelers and trip types processed with the system, and 3) save the Federal Government money. By clearly defining the strategic objectives of the effort, the delivery team can stay focused on what's important. In the absence of such a strategy, technical and policy constraints can drive product decisions.

18-F-1517//1174

Identifying Security Vulnerabilities in Department of Defense Websites – Hack the Pentagon

The Challenge

The Department of Defense (DoD) spends billions of dollars every year on information security. However, the DoD had not yet taken advantage of a "bug bounty" approach to identifying security vulnerabilities that has gained traction in the private sector.

In this "bug bounty" approach, private citizens and organizations are invited to probe specific services for potential security vulnerabilities, and are rewarded for qualifying vulnerabilities they uncover and responsibly disclose to the sponsoring organization. In this way, private citizens are provided a legal way to disclose potential vulnerabilities without fear of retaliation or prosecution, and are given an incentive for doing so. Private sector companies have successfully used this approach to improve the security of their systems. Despite this technique's acceptance as an industry best practice, the government had not attempted such an initiative before.

Project Impact Summary

- In January 2016, the Digital Service team at DoD (Defense Digital Service) got approval for the Hack the Pentagon program, inviting private citizens to find and get rewarded for uncovering vulnerabilities in its information security system.
- This "bug bounty" approach mirrors that used by companies like Facebook and Twitter to catch more vulnerabilities and cost-effectively improve security.
- DoD contracted HackerOne – a well-known bug bounty platform startup with a strong reputation in the hacker community – to run the program.
- The digital services team, in conjunction with the existing vendors, worked in near real-time to fix security flaws as they were disclosed.
- The program led to the resolution of 138 previously unidentified vulnerabilities and cost $150,000. Contracting an outside firm to do a similar audit would have cost an estimated $1M and possibly still would not have provided the same security coverage.
- In June, the Secretary of Defense announced that DoD would run a persistent bug bounty program, and efforts are being made to share the practice with other agencies. There are also additional bug bounties the DoD will be running through the month of December.

18-F-1517//1175

The Solution

On April 18, 2016, the DoD, supported by the USDS' Defense Digital Service team, launched the first bug bounty in the history of the Federal Government. This innovative effort adopted from the private sector provided authorization to security researchers – "hackers" – to attempt to hack limited public-facing DoD systems and report vulnerabilities in exchange for financial rewards. This crowdsourced solution used the talent of over a thousand individuals, 250 of whom submitted at least one vulnerability report. Of these, 138 vulnerabilities were determined to be legitimate and unique. These had escaped notice from previous penetration tests DoD conducted. Using this information, DoD resolved all of the vulnerabilities.

While the program was underway, the Defense Digital Service team held daily calls with all agency stakeholders for everyone's situational awareness in regards to bounty activities. There was also a pre-determined escalation process in place to follow in case of an immediate, critical need for defensive action against out-of-scope activity.

For the first challenge, the DoD contracted with HackerOne, an experienced administrator of bug bounty programs that performs services for companies such as Yahoo, Square, and Twitter. This strategy worked well for several reasons: HackerOne already had a strong reputation and relationship with the hacker community, they could quickly sub-contract a private background check firm, they receive and triage vulnerability reports, and they are able to allocate payouts for qualifying bounties. Using a third party platform also served to quell any concerns of hackers about providing personal information to the DoD as part of a larger effort to create a hacker database.

The cost of the program was $150,000. DoD estimates hiring an outside firm to perform a comparable security audit and vulnerability assessment would have cost more than $1 million.

18-F-1517//1176

In early June, Secretary of Defense Ash Carter announced his plan to launch a persistent DoD Bug Bounty program to continue to allow hackers to be paid for discovering security flaws in specific DoD websites, applications, binary code, networks, and systems. To make this possible, he had the Defense Digital Service take on three initiatives: run more bug bounty programs for other DoD components in 2016; develop a Vulnerability Disclosure Policy that would firmly and clearly express that hackers are acting legally when they surface DoD vulnerabilities; and provide guidance for the future acquisition of services like those provided by HackerOne.

To date, two new bug bounty programs are in the planning stages. The disclosure policy has been drafted, circulated, and is on track for release by the end of 2016. Acquisition guidance is in progress. The contract with HackerOne has been renewed, and is a model for future contracts not just at DoD, but government-wide. Altogether, these efforts will help the Defense Digital Service work with interagency teams to advise on implementing similar bug bounty programs. There will also be a "Government Only" day for agency stakeholders to gather and gain insight on Hack the Pentagon's model of success.

Success Criteria

Success Criteria	Status
Engage the hacker community.	Complete. 1,400 Registered Participants

18-F-1517//1177

Success Criteria	Status
Identify and fix previously unknown security vulnerabilities.	Complete. 138 vulnerability reports were determined to be legitimate, unique and actionable for remediation. DoD fixed all vulnerabilities identified.
Resolve vulnerabilities at a cost lower than would be possible with other methods.	Complete. The total contract cost was $150,000, with approximately half of this paid as bounties to participants. With 138 actionable vulnerability reports, that equates to less than $1,100 per vulnerability. DoD estimates it would have cost $1M for an outside firm to perform a similar security audit.

Milestones

- January 2016: Hack the Pentagon program approved.
- March 2016: Contract signed to start the program.
- April 2016: Challenge start date and bounty start date.
- May 2016: Bounty end dates.

The Process and Lessons Learned

1. **Provide a method for outside individuals to responsibly disclose security vulnerabilities.** Many private citizens have an interest in uncovering security issues. Private sector companies often provide such individuals a legal, secure way to disclose vulnerabilities without fear of retaliation or prosecution. Hack the Pentagon has shown that the "bug bounty" approach can work well for the government. Even if there is no active bug bounty program, providing researchers a way to provide responsible disclosure of vulnerabilities could yield results.

2. **Ensure the agency is prepared to remediate vulnerabilities as they are discovered, in near real-time.** DoD took the important step of putting a team

18-F-1517//1178

on standby that could implement fixes to the vulnerabilities as they were disclosed. Being able to quickly address issues helped ensure no malicious activity could take place.

3. **Involve stakeholders early.** Running a new type of program in government can be complicated. The Defense Digital Service team worked closely with the DoD Office of General Counsel to resolve legal questions around bug bounty payments, participant background checks, and whether bounties could be paid to U.S. Government personnel.

18-F-1517//1179

Section 3

Other USDS Initiatives

18-F-1517//1180

Hiring Top Technical Talent

The Challenge

In order to deliver on the mission of transforming the country's most important digital services, the Federal Government needs an infusion of modern software engineering, design, and product management skills. As demonstrated in earlier sections of this report, pairing individuals with these skills with dedicated civil servants across the Federal Government can dramatically accelerate modernization efforts on major IT acquisition projects.

However, hiring individuals with these skills has been challenging for the Federal Government for several reasons:

- It is difficult to attract highly qualified applicants to apply for government technology positions.
- The Federal Government often provides a candidate experience that is not competitive with the private sector in terms of timeline, ease of application, and frequent communication of application status.
- It is challenging to properly evaluate these highly specialized and technical skills in order to select the most qualified individuals from among all applicants.

One of the early priorities of the USDS was to build a robust recruitment and hiring program that could address these challenges.

Project Impact Summary

- It is difficult to attract highly qualified applicants from the private sector to apply for government technology positions, as the technology industry is one of the most competitive in the world.
- USDS partnered with OPM to secure the tools necessary to recruit and hire the country's brightest technical talent.
- Mirroring technology industry best practices, USDS built an experienced recruiting team who sources software engineering, product management, and design professionals from industry.
- USDS provides candidates with an easy application process and a fast timeline for hiring decisions, averaging 34 business days from application to conditional offer.

18-F-1517//1181

- USDS hiring process has a satisfaction score of 4.5 or greater (out of 5.0) from among all finalists, including those who did not receive offers.
- USDS uses subject matter experts to evaluate specialized skills.
- USDS has shortened the personnel security process from 67 days to 20 days.
- USDS reached its goal of recruiting 200 digital service experts by the end of 2016, ahead of schedule.

The Solution

USDS partnered with OPM to secure the tools necessary to recruit and hire the country's brightest technical talent. Using these tools, we created a recruiting and hiring operation that draws on several private sector best practices.

- **Engage in Targeted Recruiting Activities**. Mirroring private sector best practices, USDS has built an experienced recruiting team tasked with identifying and encouraging a diverse set of qualified applicants to apply for digital service positions. Specific tactics include targeted outreach to technology and design professionals (including those who are not currently seeking a new job), events, roundtables, and building a network of influencers who can validate the importance and professional respectability of the USDS' public service mission.

- **Focus on Candidate Experience**. The USDS hiring process puts a premium on providing a high quality candidate experience that is competitive with the private sector. Specifically, the USDS aims to provide candidates with an easy application process (currently delivered via the website), a fast timeline for hiring decisions (targeting 15 business days from application to conditional offer for qualified applicants), and good visibility into the process and application status.

  USDS measures its effectiveness by asking all candidates who complete the hiring process to complete a satisfaction survey, and target a satisfaction score of 4.5 or greater (out of 5.0) from among all finalists (including both those who receive offers and those who do not).

- **Use Subject Matter Experts to Evaluate Specialized Skills.** Evaluating applicants with highly specialized skills is a challenging practice that requires subject matter expert involvement at every stage. USDS has fully embraced the use of such experts in the hiring process. Each candidate for the USDS is evaluated by a panel of engineers, designers and product managers who themselves possess the desired specialized skills. By ensuring that applicants are evaluated by technical specialists within their own discipline, the process ensures

18-F-1517//1182

that individuals selected for USDS roles have the digital expert skills that are required to improve government technical services.

This hiring program is run centrally from the USDS headquarters unit inside OMB, so that all chartered USDS teams can benefit from a dedicated recruiting operation and a standardized, rigorous selection process.

Success Criteria	Status
Hire 200 Digital Service Experts by end of 2017	On track to meet target ahead of schedule. 196 Digital Service Experts hired as of September 2016.
Days from Application to Conditional Offer = 15 business days	In progress. Time reduced from 55 days in Q4 2015 to 34 days in Q3 2016.
Day from Conditional Offer to Final Offer (personnel security process) = 16 days	In progress. Time reduced from 67 days in Q4 2015 to 20 days in Q3 2016.
Candidate Satisfaction Score for going through the hiring process is 4.5 (or above) out of a scale from 1 to 5 (5 being the most satisfied)	On track. Average candidate satisfaction since Q4 2015 is greater than 4.5.

18-F-1517//1183

Transforming Federal IT Procurement

The Challenge

Government procurement cycles do not keep pace with fast-changing technology and user needs. This is largely due to a reliance on waterfall development methods where requirements are defined and documented in full detail before any design, development or user testing can take place. When tied to inflexible contracts, this approach makes it very difficult to build an easy to use, effective digital service. Adapting patterns and best practices from private industry will allow the Federal Government to deliver products faster, cheaper, and at higher quality.

Project Impact Summary

- The USDS procurement team has launched several projects to help the Federal Government enter into better, more agile contracts and buying decisions.
- The objective is not only to change the way IT services and products are acquired, but to model new procurement processes for the government at large.
- During a discovery sprint, the USDS team made recommendations for modernizing SAM.gov, the system businesses use to receive contracts and grants from the Federal Government.
- The GSA has accepted the recommendation to move SAM.gov to a Common Services Platform, allowing developers to make speedier improvements to the existing system, automate more services, and increase security.
- USDS also advised SBA to consolidate certification systems for small businesses seeking government contracts. SBA has since moved to a modern technology stack, and will soon process all certifications through certify.sba.gov.
- In October 2015, USDS and OFPP launched the Digital IT Acquisition Professional Training (DITAP) program, piloting a course that successfully taught federal contracting professionals material relevant to digital services procurement.
- USDS and OFPP are now working to transition this program to GSA and other Federal Government agencies.
- Also in partnership with OFPP, USDS developed the TechFAR Handbook, and the TechFAR Hub, to advise all federal agencies on how to adopt more flexible acquisition practices.

18-F-1517//1184

The Solution

USDS has a dedicated acquisition team working to improve the government technology marketplace and to help the government make better buying decisions. The USDS procurement team has launched several solutions since its inception and continues to evaluate new potential solutions.

System for Award Management (SAM.gov)

In order for businesses to receive a contract or grant from the government, they are required to register in the General Services Administration's (GSA) System for Award Management (SAM.gov). However, because the process is so cumbersome, many businesses are discouraged from engaging with the government. The USDS and GSA completed a two-week discovery sprint in March 2016 to define what a successful SAM.gov modernization would look like. This included evaluating the technology, business processes, and the customer experience underlying SAM and the related Integrated Award Environment.

USDS' recommendations from the discovery sprint included:

- **Shift from Process to Product.** In order to develop and ship such a large solution, the work must be centered around the idea that it is delivering a federal-wide product capable of meeting the demands and objectives of various and competing end user needs.
- **Invest in the Team.** Rather than hiring external experts, or bringing on other teams, GSA should make an investment in and prioritize comprehensive and frequent training for all roles within its Integrated Award Environment, from management to external stakeholders to contracting officers.
- **Empower a New Team Culture.** The unified team has the potential to deliver a powerful digital service by adopting a culture that embraces change, challenges the status quo, and does not accept anything less than excellence. The ideal team is self-motivated to look at everything as an opportunity to solve end users' problems.
- **Deliver. Deliver. Deliver.** The main benefit for adopting an agile development methodology is the ability to accelerate product delivery. Leadership must dissolve any fears of failure that create hesitancy when making a change to a product—whether it's prototypes, beta versions, or enhancements. The team has universally expressed a willingness to move to continuous integration, rapid delivery model, and USDS provided a 6-month plan for this transition.

18-F-1517//1185

- **Migrate to a Secure, Robust Services Platform.** The SAM.gov environment is transitioning to a Common Service Platform that will allow applications to be built on top of an infrastructure layer. Adopting continuous integration, implementing the "DevOps" practice of integrating system operations with application development teams and processes, and establishing protocols for a multi-vendor environment to implement changes on the new platform would speed improvements. In addition, there should be a drive to automate services and provide real-time data, such as TIN validation. To improve security, USDS recommended SAM.gov implement host segmentation and network security controls for restricting access to sensitive data on the Secure FTP service. Other key areas of opportunity recommended to improve the basic platform include open-source, standardization, and implementing a mitigation strategy for DDoS protection aligned with the public release of services on the Common Service Platform (CSP).

GSA has accepted the recommendations and is in the process of making nearly all of the changes. They have already restructured their team based on functions and are working cohesively in a team based environment.

Small Business Certifications

It is part of the mission of the Small Business Administration to expedite small businesses' access to government contracts. Better utilization of the 8(a) Business Development, Women-Owned Small Business (WOSB), HUBZone, and Service Disabled Veteran Owned Small Business Programs would serve this mission.

In early 2015, SBA asked the USDS to help it modernize and consolidate the systems that power these certification programs. After USDS personnel conducted an initial technical evaluation, the USDS procurement team assisted SBA in developing a contract to create a modern system using the best practices described in the Digital Services Playbook. SBA has since awarded an agile software development contract for revamping these certification processes as part of the SBAOne project.

In just 5 months following the award of the contract, SBA moved to a modern technology stack, hosted on flexible public cloud infrastructure, and launched an eligibility service in December 2015 for the WOSB program. This release was shortly followed by the successful launch of the modernized Woman-Owned Small Business certification system in March 2016 on certify.SBA.gov. Work is underway for the modernization of the 8(a) certification program, for a release planned in early 2017. Eventually all SBA Certifications will be processed through Certify.SBA.Gov.

18-F-1517//1186

Digital IT Acquisition Professional Training (DITAP)

Helping the government become smarter buyers requires the establishment of a specialized and educated procurement workforce that understands the digital and IT marketplace, utilizes best practices for IT purchasing, and capitalizes on the power of the government acting as a single purchasing entity and the economies of scale this provides. To achieve this, the USDS and the Office of Federal Procurement Policy (OFPP) have partnered to develop a digital IT acquisition professional community (DITAP).

The first component of this community was a training and certification program for contracting officers. USDS and OFPP posted a prize competition on Challenge.gov in May 2015 to develop the Digital Service Contracting Professional Training and Development Program for the Federal Government. As a part of this process, USDS and OFPP held a Reverse Industry Day where 70 representatives from vendors familiar with agile software development techniques, system integrators, collegiate entities, and training developer came together to confirm that the specific training did not yet exist and confirm that the Challenge.gov platform would be an effective path forward in developing the training. In all, 23 submissions were received, 3 finalists provided mock classroom presentations of their content and assessment plan, and by October 2015, the final winner began its finalized 6-month course with the first class of 30 Contracting Professionals from 20 federal agencies.

Over the 6 months, the attendees completed 11 days of classroom training on agile software development methodology, cloud hosting, and the "DevOps" practice of integrating system operations with application development teams and processes. The attendees completed 120 hours of self-directed learning and webinars, heard from 10 guest speakers, supported 6 live digital assignments, and completed a final capstone assessment of skills. Since the course ended in March 2016, 6 participants received promotions or changed job roles to take on IT work, 12 participants were assigned digital service acquisition work or are working with an agency digital service team, and two were named agency Acquisition Innovation Advocates. 90% of the 28 graduates felt they were ready to conduct digital service acquisitions in their agency. USDS and OFPP are restructuring the next round of implementation based on these results. The second class began in July 2016.

USDS and OFPP are currently training Federal Acquisition Institute (FAI) facilitators on how to conduct the program, for transfer of responsibilities in FY17. In addition, USDS and OFPP are finalizing the Federal Acquisition Certification in Contracting (FAC-C) Digital Service certificate program requirements and encouraging the development of similar training programs for government Contracting Officer Representatives and Project Managers. The long-term goal is for any federal training institution to be able to

18-F-1517//1187

use and update the course material in an open source manner to create their own development program without incurring the cost of content.

Success Criteria	Status
60 Contracting Officers trained in digital service acquisition.	In progress. 28 completed pilot. 30 started next round in July 2016

TechFAR Handbook

In the Government, digital services projects too often fail to meet user expectations or contain unused or unusable features. Several factors contribute to these outcomes, including, overly narrow interpretations of what is allowed by acquisition regulations. The Office of Federal Procurement Policy, with the assistance of the USDS, developed the TechFAR to highlight flexibilities in the Federal Acquisition Regulation (FAR) that can help agencies implement "plays" in the Digital Services Playbook.

The TechFAR is a handbook that describes relevant FAR authorities and includes practice tips, sample language, and a compilation of FAR provisions that are relevant to adopting an agile style of software development as the primary means of delivering software solutions. Agile software development is a proven commercial methodology characterized by incremental and iterative processes where releases are produced in close collaboration with the customer. The TechFAR facilitates a common understanding among agency stakeholders of the best ways to use acquisition authorities to maximize the likelihood for success in agile contracts and there is nothing prohibitive in the Federal Acquisition Regulations for adopting these methods and re-engineering contracts to support delivery of quality products. This handbook is a living document; users are urged to provide feedback, share experiences, and offer additional strategies, practice tips, policies, or contract language that may be used to assure that IT acquisitions achieve their desired results.

USDS also released the TechFAR Hub on GSA's Acquisition Gateway. The TechFAR Hub is designed to advise all federal agencies on how to implement best practices, as described in the digital service playbook and TechFAR, and as a community space for digital service practitioners.

18-F-1517//1188

Supporting the Development of Federal Shared Services

Shared technology platforms and services have the potential to simplify government products, increase consistency, reduce development costs, and eliminate duplication. Security also benefits by focusing resources on a smaller number of key components.

USDS is uniquely positioned to support the development of these shared services, because it works across many agencies and has visibility into many of the government's digital service development efforts. This insight enables USDS to invest in developing and promoting reusable platforms and services.

Project Impact Summary

- USDS supports the development of shared technology platforms and services because they have the potential to simplify government products, increase consistency, and reduce development costs.
- In May 2016, a USDS and 18F team began implementation work on Login.gov, a service that will provide a secure and user-friendly login process for multiple government digital services. Login.gov is currently being integrated with its first agency customer.
- Many government digital services are siloed under unique brands and programs, leading agencies to spend time and money redesigning common digital components such as buttons, forms and search bars. In September 2015, USDS and 18F released the U.S. Web Design Standards, a set of components that agencies can adopt to provide their users a consistent, high quality online experience while reducing the chance of duplicative work. Moving forward, GSA will continue to develop the Standards. Since its release, the standards have been downloaded over 17,000 times.

Login.gov Consumer Identity Platform

Many consumer-facing government digital services require individuals to create user accounts in order to access the service. The USDS has helped several agencies implement such systems, including at USCIS, CMS, SBA and IRS. Many more agencies have already implemented their own solutions. Despite several earlier attempts to build a common identity management platform, no such platform has been widely adopted.

18-F-1517//1189

Providing a secure and user-friendly login process for the government's digital services would improve the experience of interacting with government services, and help agencies implement digital services faster and more securely. To that end, the USDS and the General Service Administration's 18F are working iteratively with a team of technologists from across the Federal Government to build a platform for users who need to log in to government services. The team is coordinating with the Federal Acquisition Service, the Office of Management and Budget, and the National Institute of Standards and Technology on the specifics of the platform.

To build the Login.gov platform, the team is using modern, user-friendly, strong authentication and effective identity proofing technology. The project builds off of the hard work that was already done to create and implement the Connect.gov pilot, an earlier project with similar goals. The team is also using lessons learned from our counterparts in the UK who built GOV.UK Verify. More specifically, the team will accomplish these goals by:

- Creating a simple, elegant way for the public to verify their identity, log in to federal government websites, and, if necessary, recover their account
- Building experiences, processes, and infrastructure that will use the latest available technology to safeguard all user data
- Delivering software that will allow government developers to integrate it within hours, not weeks
- Iteratively improving the system throughout its lifetime
- Preserving privacy including mitigating risks and adhering to federal privacy guidelines
- Following security best practices including implementing easy-to-use multi-factor authentication

The team has identified the first agency to adopt this shared platform, and is in talks with several additional agency customers to be the second adopter early in 2017. Based on the success of the first two initial adopters, the team will scale out the adoption in 2017.

U.S. Web Design Standards

When members of the public access government services online, they're often met with confusing navigation systems, conflicting visual brands, and inconsistent interaction patterns — all factors that can erode trust in our government's services.

18-F-1517//1190

A snapshot of buttons across government websites

Recognizing the necessity of consistent, easy-to-use design, many agencies have started creating their own design patterns and user interface (UI) toolkits, but their efforts are often duplicative. Because many digital services are siloed under unique brands and programs, the Federal Government runs the risk of spending time and money reinventing the wheel — that is, recreating common patterns such as buttons, forms, and search bars that already exist. What's more, creating pattern libraries and toolkits is a time- and labor-intensive process, and one not all agencies have the resources to support.

Designers and developers at USDS and 18F teamed up to address the need for consistent, accessible design components. Together, they created the Draft U.S. Web Design Standards (the "Standards"), a set of open source UI components and a visual style guide that agencies can use to create consistent online experiences. The Standards, which launched in September 2015, follow industry-standard accessibility guidelines and draw on the best practices of existing style libraries and modern web design. To offer the highest-quality product, the Standards team makes frequent updates to introduce new features, fix bugs, provide clearer documentation, and more.

Agencies using the Standards enjoy several distinct benefits. Not only are they providing an enjoyable, consistent user experience, but they're also saving design and development time that can be dedicated to other projects. Using the Standards, a team can build a site quickly and with minimal effort, allowing their agency to communicate its message more effectively.

18-F-1517//1191

Moving forward, GSA's 18F team will continue to develop the Standards.

Success Criteria	Status
Overall Goal: Begin implementation of at least one outstanding common platform by end of 2016.	Complete. Implementation of shared login platform began in May 2016. Draft U.S. Web Design Standards released September 2015.
Sub-Goal: Draft U.S. Web Design Standards available for agency use.	Complete. Initially released in September 2015, they include an online style guide and downloadable software package. The standards have been downloaded more than 17,000 times. As of September 2016, more than 78 people have contributed to the Standards' code base, and more than 200 people have participated in conversations on the Standards' GitHub repository. The Standards team welcomes outside recommendations and contributions, which help drive the project's process forward.
Sub-Goal: At least three agencies have adopted a shared login service.	Incomplete. Development of an interagency login system is in progress, but it is not in use yet. Initial agency customer identified.

Milestones

Web Design Standards

- September 2015: Draft U.S. Web Design Standards released

Consumer Identity Platform

- December 2015: Identity sprint completed

18-F-1517//1192

- January 2016: Research starts
- May 2016: Implementation begins

18-F-1517//1193

Exhibit 37

U.S. tells Arkansas to delete files on voter data

By Bill Bowden , Brian Fanney twitter
This article was published today at 4:30 a.m.

0

Comments (8) Font Size

Arkansas voter data provided to President Donald Trump's voter-fraud commission is headed for the trash days after it was submitted.

According to an email exchange obtained Wednesday under the state Freedom of Information Act, Andrew Kossack, associate counsel for Vice President Mike Pence, asked officials in Secretary of State Mark Martin's office to delete from a federal server the voter data it submitted.

However, state officials could not access the server.

"We were unable to access the SAFE site again in order to pull down the file, pursuant to your request," wrote Peyton Murphy, assistant director of the state elections division, in a Monday email. "We understand that the file has not yet been accessed, but that it will expire 14 days from the time of the upload."

Kossack replied that the federal site would delete the file.

"I'll be back in touch with next steps," he continued. "Again, thank you for your submission, and my apologies for this inconvenience."

ADVERTISING

18-F-1517//1195

Arkansas submitted its data on July 5. It was the first state to submit data to the Presidential Advisory Commission on Election Integrity.

The SAFE site -- also known as the Safe Access File Exchange -- is at the heart of a lawsuit filed by the Washington, D.C.-based Electronic Privacy Information Center. The file exchange is run within the Department of Defense.

Kossack referred to the lawsuit in his email.

[EMAIL UPDATES: Get free breaking news alerts, daily newsletters with top headlines delivered to your inbox]

The Electronic Privacy Information Center contends that the commission failed to conduct a privacy information assessment -- required under the E-Government Act of 2002 -- before collecting the data using the Department of Defense system.

"The 'SAFE' URL, recommend by the Commission for the submission of voter data, leads election officials to a non-secure site," according to the Electronic Privacy Information Center.

"Regarding this website, Google Chrome states: 'Your connection is not private. Attackers may be trying to steal your information from [the site proposed by the Commission] (for example, passwords, messages, or credit cards).'"

In the initial request for information, dated June 28, Kris Kobach, vice chairman of the Presidential Advisory Commission on Election Integrity, noted that the commission wanted Arkansas data -- "if publicly available under the laws of your state" -- including names, addresses, dates of birth, political party affiliations, the last four digits of Social Security numbers "if available," voter history, voter status, felony convictions, information regarding voter registration in another state, military status and overseas citizen information.

The information submitted to the file exchange from Arkansas did not contain Social Security numbers, felony convictions, military status and driver's license numbers. Such information is not publicly available in Arkansas.

However, names, addresses, dates of birth, political party affiliations, voter history since 2008, registration status, email addresses and phone numbers -- were shared. The database does not say for whom someone voted -- only whether they voted.

The same Arkansas voter information that was released to the Trump administration has been provided about 200 times since January 2015 to various entities, Kelly Boyd, chief deputy secretary of state, told legislators and county clerks meeting Wednesday in Eureka Springs.

Those entities include states, organizations, political parties and Arkansas legislators, he told a crowd of about 100 at the Basin Park Hotel.

"We submit information every year to the state cross-check program, and we do that at no charge," Boyd said. "And we did that at no charge for this program."

"To be very clear on this, there was no sensitive information released, no Social Security numbers, no partials, no military data, no felon data, no data that you can't get out of the phone book."

Boyd said the data would reveal some voting information.

18-F-1517//1196

"They're going to know whether you voted R or D or O [optional] or N for nonjudicial in the primaries," said Boyd. "It would tell whether you voted E early, A absentee or P at the polls, back to 2008. ...

"I know there's been a lot of angst about that, and I'm sorry. I wish there hadn't been. This information is openly available. There are ways to make it not openly available. I'll work with you if you want to do that."

Gov. Asa Hutchinson told a group of high school students Monday that the state should not have provided any data to the Trump commission.

"I am not a fan of providing any data to the commission in Washington," Hutchinson said in response to a student's question.

"Even though it is publicly available information and anyone can get it -- all you have to do is file a Freedom of Information [Act] request to get the information -- I just don't want to facilitate the providing of that information to a federal database. I don't think that's helpful for us."

The governor spoke as Kossack and Arkansas secretary of state staff members were trading emails about deleting the Arkansas information.

Information for this article was contributed by The Associated Press.

Metro on 07/13/2017

Print Headline: U.S. tells state to delete files on voter data; But authorities in Arkansas unable to access federal site

Exhibit 38

DECLARATION OF MARC ROTENBERG

I, Marc Rotenberg, declare as follows:

1. I am President and Executive Director for the Plaintiff Electronic Privacy Information Center ("EPIC").

2. Plaintiff EPIC is a non-profit corporation located in Washington, D.C. EPIC is a public interest research center, which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has a particular interest in preserving privacy safeguards established by Congress, including the E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note), EPIC pursues a wide range of activities designed to protect privacy and educate the public, including policy research, public speaking, conferences, media appearances, publications, litigation, and comments for administrative and legislative bodies regarding the protection of privacy.

3. I am a member in good standing of the Bar of the District of Columbia (admitted 1990), the Bar of Massachusetts (1987), the U.S. Supreme Court (1991), the U.S. Court of Appeals—1st Circuit (2005), the U.S. Court of Appeals—2nd Circuit (2010), the U.S. Court of Appeals—3rd Circuit (1991) the U.S. Court of Appeals—4th Circuit (1992), the U.S. Court of Appeals—5th Circuit (2005), the U.S. Court of Appeals—7th Circuit (2011), the U.S. Court of Appeals—9th Circuit (2011), and the U.S. Court of Appeals—D.C. Circuit (1991).

4. I have taught Information Privacy Law continuously at Georgetown University Law Center since 1990.

5. I am co-author with Anita Allen of a leading casebook on privacy law.

6. In my capacity as President and Executive Director, I have supervised both EPIC's response to the Department's rulemaking and EPIC'S participation in all stages of litigation in the above-captioned matter.

7. The statements contained in this declaration are based on my own personal knowledge.

8. EPIC works with an Advisory Board consisting of nearly 100 experts from across the United States drawn from the information law, computer science, civil liberties and privacy communities.

9. Members of the EPIC Advisory Board must formally commit to joining the organization and to supporting the mission of the organization.

10. Members of the EPIC Advisory Board make financial contributions to support the work of the organization.

11. Members of the EPIC Advisory Board routinely assist with EPIC's substantive work. For example, members provide advice on EPIC's projects, speak at EPIC conferences, and sign on to EPIC amicus briefs.

12. In this matter, EPIC represented the interests of more than 30 members of the EPIC Advisory Board, who signed a Statement to the National Association of State Secretaries in Opposition to the Commission's demand for personal voter data.

Under penalty of perjury, I declare that the foregoing is true and correct to the best of my knowledge and belief.

Marc Rotenberg
EPIC President and Executive Director

Executed this 7th day of July, 2017

18-F-1517//1200

Exhibit 39

Trump election group backs away from its request for voter data after outcry

Commission on election integrity's 'repugnant' request for voter data prompted privacy concerns and numerous legal challenges

277

Andrew Gumbel in Los Angeles

Thursday 13 July 2017 05.00 EDT

The Trump administration is backing away from its extraordinary attempt to gather voters' personal information, following a barrage of legal challenges, an outcry from state officials, and a rash of voter registration cancellations by people concerned about their privacy.

ADVERTISING

Voting rights groups have filed at least six lawsuits in response to a letter sent out on 28 June by Kris Kobach, vice-chair of the presidential advisory commission on election integrity, asking state officials to provide names of the country's 150 million voters. In addition, the letter sought voters' addresses, social security numbers, voting histories, party affiliation, criminal histories, military status, and more.

18-F-1517//1202

Kobach has said the request is designed to help prevent fraudulent in-person voting. But his detractors say he is looking for a solution to a non-existent problem and suspect his true interest is in finding reasons to deny legitimate voters their rights, for partisan advantage.

Both Kobach and Trump have floated the notion that 3 to 5 million people voted illegally last November – a notion that has angered both Republican and Democratic election officials because there is no shred of evidence to support it.

> “ Trump’s voter fraud commission is a shameless white power grab
> Steven W Thrasher
>
> Read more

Kobach’s letter told states to comply with his request by 15 July, but the White House has already postponed that deadline pending a ruling from the Washington DC circuit court on one of the lawsuits. That ruling is not due until next week at the earliest.

The commission has also abandoned plans to store the information on a temporary Pentagon computer and promised to have a dedicated White House server ready to receive the data by next week.

Not one state – not even Kansas, where Kobach is secretary of state and in charge of elections – has agreed to comply fully with the request. Many have cited privacy concerns and other legal restraints. Only three states, Colorado, Missouri and Tennessee, have indicated any enthusiasm about complying. Many more have responded with fury, including Mississippi, whose Republican secretary of state memorably told Kobach to “go jump in the Gulf of Mexico”.

Advertisement

Maryland’s attorney general, Brian Frosh, called the request “repugnant”. “It appears designed only to intimidate voters,” he wrote, “and to indulge President Trump’s fantasy that he won the popular vote.”

According to the lawsuits filed by the Electronic Privacy Information Center (Epic), the American Civil Liberties Union (ACLU) and others, Kobach’s request sidestepped clear legal requirements on privacy protection – the issue that prompted the White House to hold off on its deadline.

The suits also accuse the commission of working at a constitutionally intolerable level of secrecy, and Kobach himself of blurring the legal lines between his position as vice-chair and his candidacy in next year’s Kansas gubernatorial election.

Epic’s complaint and call for a temporary restraining order, filed this month, denounced the proposed voter database as “unnecessary and excessive” and said the commission risked violating “the informational privacy rights of millions of Americans” and exposed the country’s electoral system to potential new forms of registration and voter fraud. To make the information gathered by the commission public, it added, would be “both without precedent and crazy”.

Donald and Melania Trump cast their votes in the 8 November 2016 presidential election. Photograph: Evan Vucci/AP

Two of the suits, by the ACLU and the Lawyers' Committee of Civil Rights Under Law, seek to postpone the presidential committee's next meeting, set for next Thursday, unless the White House discloses its communications about the meeting and opens it to the public.

Advertisement

Voting rights activists are hoping that the legal and political pressure will induce the White House to drop the data-gathering exercise altogether. "The program was ill conceived and poorly executed," Epic's president and executive director Marc Rotenberg said in a statement. "We expect the commission will simply announce that it has no intention, going forward, to ask the states for their voter records."

Some damage, however, has already been done, as election officials in at least four states – Arizona, Colorado, Florida and North Carolina – report receiving requests from hundreds of voters to cancel their registrations to protect their personal information.

Local voting officials were bombarded with email requests and phone calls after the Kobach letter became public. In some cases, the officials talked voters out of cancelling their registrations, arguing that the data was in the system already and they would only be damaging themselves. In other cases, voters said straight out they did not trust the presidential commission. One North Carolina voter said it "smells funny".

The voter response in Arizona appears to have triggered a change in policy. The secretary of state there initially said she would be withholding social security numbers, dates of birth and other identifying details but otherwise complying with the request. By the time she sent her official response, however, the line had changed to a flat no.

18-F-1517//1204

Exhibit 40

Arkansas Voter Registration Data

The Arkansas Secretary of State's Office provides three different statewide voter registration data files.

The first is the statewide Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted.

The second file contains the Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle. The older elections are incomplete since some counties did not enter voter results into the previously used VR databases. The Vote History file does not contain voters' names and therefore must be linked to the Voter Registration file by a unique Voter ID # found within each file.

The third file is a combination of the Voter Registration and Vote History files (VRVH).

- All files are ASCII text files with comma delimited, double quoted fields. This is commonly called comma-separated values format or .CSV format.
- Since there are about 1.6 million records in each, the files will not fit into an Excel spreadsheet.
- The VR file size is about 585 MB, the Vote History file size is about 402 MB, and the Combo file is about 1 GIG. Due to the file size no files can be sent via email.
- The cost per file is $2.50.
- The file(s) are available in CD format for pickup at the State Capitol Building or by mail. These files can also be placed on an FTP site if desired.

We are often asked the question, "Are there any restrictions on the use of this data?"
Currently there are no state laws that place restrictions on the use of data that we release. However, there are Federal and State laws that restrict some fields on the VR record from being released (Arkansas Code, Amendment 51§ 8(e)). These fields are never released and are never on any file that our office provides to the public.

To request a file you may complete the Data Request Form on the following page.

18-F-1517//1206

Data Request Form

Date: _____ Request taken by: _____

Contact Name: _____ Telephone: _____

Email Address: _____

Please check one of the following: Do you wish to...

Pick up the data ____ ***Have the data placed on your FTP site____***
Have the data mailed to the address below ____

Company: _____

Address: _____

City, State, Zip: _____

Data Requested, Comments and Instructions: _____

_____

_____

_____

_____

Number of Data Disk(s)/File(s)/Report(s) created: _____ created by: _____
Data Disk(s) filename(s): _____

_____

Please remit $2.50 for each enclosed Data Disk(s)/File(s)/Report(s)

Number of Data Disk(s)/File(s)/Report(s) created: _____ Total Cost:_____

Make Check or Money Order payable to: **Arkansas Secretary of State**

Mail payment to: ATTN: Data Request
Arkansas Secretary of State
State Capitol Bldg, Room 026
Little Rock, AR 72201

Any questions regarding this data should be reported to the Office of the Secretary of State at 1-800-247-3312 or via email at voterservices@sos.arkansas.gov .

18-F-1517//1207

Exhibit 30

Illinois Voter Registration System Database Breach Report

The Illinois State Board of Elections was the victim of a malicious cyber-attack of unknown origin against the Illinois Voter Registration System database (IVRS) beginning June 23, 2016. Because of the initial low volume nature of the attack, SBE staff did not become aware of the breach until the volume dramatically increased on July 12th. At that point, SBE IT immediately took measures to stop the intrusion. In the following weeks, SBE staff worked to determine the scope of the intrusion, secure databases and web applications, comply with state law regarding personal information loss, and assist law enforcement in their investigation of the attack.

Analysis concluded that in addition to viewing multiple database tables, attackers accessed approximately 90,000 voter registration records.

Timeline

July 12, 2016

State Board of Elections IT staff was made aware of performance issues with the IVRS database server. Processor usage had spiked to 100% with no explanation. Analysis of server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of the Paperless Online Voter Application (POVA) web site. Additionally, the server logs showed the database queries were malicious in nature – a form of cyber-attack known as SQL (Structured Query Language) Injection. SQL Injections are essentially unauthorized, malicious database queries entered in a data field in a web based application. We later determined that these SQLs originated from several foreign based IP addresses.

SBE programmers immediately introduced code changes to eliminate this vulnerability.

July 13, 2016

SBE IT took the web site and IVRS database offline to investigate the severity of the attack.

Analysis of the web server logs showed that malicious SQL queries had begun on June 23, 2016.

SBE staff maintained the ability to log and view all site access attempts. Malicious traffic from the IP addresses continued, though it was blocked at the firewall level. Firewall monitoring indicated that the attackers were hitting SBE IP addresses 5 times per second, 24 hours per day.

SBE staff began working to determine the extent of the breach, analyzing the integrity of the IVRS database, and introducing security enhancements to the IVRS web servers and database.

July 19, 2016

We notified the Illinois General Assembly of the security breach in accordance with the Personal Information Protection Act (PIPA). In addition, we notified the Illinois Attorney General's office.

18-F-1517//1209

July 21, 2016

SBE IT completed security enhancements and began bringing IVRS back online.

July 28, 2016

Both the Illinois Voter Registration System and the Paperless Online Voter application became fully functional.

Ongoing

SBE IT staff continues to monitor its web server and firewall logs on a daily basis.

Outside Agency Participation

As a result of informing the Illinois Attorney General's office of the breach, the SBE was contacted by the Federal Bureau of Investigation. We have fully cooperated with the FBI in their ongoing investigation.

The Illinois Department of Innovation and Technology (which is a State-wide entity that coordinates the IT systems of the various State agencies) was helpful by providing web traffic logs and assisting with web server log analysis.

The FBI advised that we work with the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT) to ensure there was no ongoing malicious activity on any of SBE's systems.

PIPA Compliance

Nearly 76,000 registered voters were contacted as potential victims of the data breach.

The SBE provided these individuals information on steps to take if they felt they were the victims of identity theft. Additionally, the SBE developed an online tool to inform affected individuals of the specific information included in their voter record.

Future Concerns

Voting Equipment – One of the concerns facing our state and many others is aging voting equipment. The Help America Vote Act (HAVA) established requirements for voting equipment, but, while initial funding was made available, additional funding has not been appropriated.

In addition to future funding, HAVA restrictions on spending could be relaxed to allow spending on enhanced security across all election-related systems.

New Standards for Voting Equipment

Security Training and Guidance for State and Local Election Officials – Cyberattacks targeting end users are of particular concern. Security training funded and provided by a federal entity such as the EAC would be beneficial. In addition, any guidance or recommendations as to methods for the protection of registration and voting systems from cyber intrusions are always welcome.

18-F-1517//1210

Exhibit 31

Report Information from ProQuest

July 12 2017 17:47

18-F-1517//1212

Table of contents

18-F-1517//1219

S INTEL HEARING ON RUSSIAN INTERFERENCE IN 2016 ELECTION, PANEL 1

Publication info: Political Transcript Wire ; Lanham [Lanham]21 June 2017.

ProQuest document link

Links: Check SFX for Availability

Full text: (CORRECTED COPY - CORRECTIIONS THROUGHOUT TEXT)

S Intel Hearing on Russian Interference in 2016 Election, Panel 1

JUNE 21, 2017

SPEAKERS: SEN. RICHARD M. BURR, R-N.C. CHAIRMAN SEN. JIM RISCH, R-IDAHO SEN. MARCO RUBIO, R-FLA. SEN. SUSAN COLLINS, R-MAINE SEN. ROY BLUNT, R-MO. SEN. TOM COTTON, R-ARK. SEN. JAMES LANKFORD, R-OKLA. SEN. JOHN CORNYN, R-TEXAS SEN. MARK WARNER, D-VA. VICE CHAIRMAN SEN. RON WYDEN, D-ORE. SEN. MARTIN HEINRICH, D-N.M. SEN. JOE MANCHIN III, D-W.VA. SEN. KAMALA HARRIS, D-CALIF. SEN. DIANNE FEINSTEIN, D-CALIF.

SEN. ANGUS KING, I-MAINE

SEN. JACK REED, D-R.I.

WITNESSES: SAM LILES, ACTING DIRECTOR, OFFICE OF INTELLIGENCE AND ANALYSIS CYBER DIVISION DEPARTMENT OF HOMELAND SECURITY

JEANETTE MANFRA, UNDERSECRETARY OF HOMELAND SECURITY, AND ACTING DIRECTOR, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

BILL PRIESTAP, ASSISTANT DIRECTOR, FBI COUNTERINTELLIGENCE DIVISION

[*] BURR: Today the committee -- committee convenes it's sixth open hearing of 2017, to further examine Russia's interference in the 2016 elections. This is yet another opportunity for the committee and the American people to drill down on this vitally important topic.

In 2016 a hostile foreign power reached down to the state and local levels to touch voter data. It employed relatively sophisticated cyber tools and capabilities and helped Moscow to potentially build detailed knowledge of how our elections work. It was also another example of Russian efforts to interfere into a democracy with the goal of undermining our system.

In 2016, we were woefully unprepared to defend and respond and I'm hopeful that we will not be caught flatfooted again.

Our witnesses are here to tell us more about what happened in 2016, what that tells us about Russian intentions, and what we should expect in 2018 and 2020. I'm deeply concerned that if we do not work in lockstep with the states to secure our elections, we could be here in two or four years talking about a much worse crisis.

The hearing will feature two panels.

First panel will include expert witnesses from DHS and FBI to discuss Russian intervention in 2016 elections and U.S. government efforts to mitigate the threat.

The second panel will include witnesses from the Illinois State Board of Elections, the National Association of State Elections and Directors, National Associations of Secretary of States and an expert on election security to give us their on-the-ground perspective on how federal resources might be brought to bear on this very important issue.

For our first panel, I'd like to welcome our witnesses today: Dr. Samuel Liles, acting director of Cyber Division within the Office of Intelligence and Analysis at the Department of Homeland Security; Jennifer (sic) Manfra, acting deputy undersecretary, National Protection and Programs Dictorate (sic), also at DHS.

And Jeanette, I think I told you next time you came I did not want "acting" in front of your name. So now I've

 18-F-1517//1214 ProQuest

publicly said that to everybody at DHS. Hopefully next time that will be removed.
And Bill Priestap. Bill's the assistant director for Counterintelligence Division at the Federal Bureau of Investigation.
Bill, I want to thank you for the help that you have personally provided to the investigative staff of this committee, as we've worked through, so far, over five and a half months of our investigation into the 2016 elections.
As you're well aware, this committee is in the midst of a comprehensive investigation on the specific issue: the extent to which Russian government under the direction of President Putin conducted intelligence activities, also known as Russian active measures, targeted at the 2016 U.S. elections. The intelligence community assesses that, while Russian influence obtained and maintained access to elements of multiple U.S. state and local election boards, those systems were not involved in vote tallying.
During the first panel, I would like to address the depth and the breadth of Russian government cyber activities during the 2016 election cycle, the efforts of the U.S. government to defend against these intrusions, and the steps that DHS and FBI are taking to preserve the foundation of our democracy's free and fair elections in 2018 and beyond.
I thank all three of our first witnesses.
I turn to the vice-chairman.
WARNER: Thank you, Mr. Chairman.
And welcome to the witnesses.
And, Bill, thank you again for all the work you've done with us.
WARNER: We all know that in January, the entire intelligence community reached the unanimous conclusion that Russia took extraordinary steps to intervene in our 2016 presidential elections. Russia's interference in our elections in 2016 I believe was a watershed moment in our political history.
This was one of the most significant events I think any of us on this dais will be asked to address in our time as senators. And only with a robust and comprehensive response will we be able to protect our democratic processes from even more dramatic incursions in the future.
Much of what the Russians did at this point, I think at least in this room, is -- was well known: spreading fake news, flooding social media, hacking personal e-mails and leaking them for maximum political benefit.
Without firing a shot and at minimal cost, Russia sowed chaos in our political system and undermined faith in our democratic process. And as we've heard from earlier witnesses, sometimes that was aided by certain candidates, in terms of their comments about the legitimacy of our democratic processes.
Less well understood, though, is the intelligence community's conclusion that they also secured and maintained access to elements of multiple U.S. state and local electoral boards.
Now, again, as the chairman has said, there's no reason to doubt the validity of the vote totals in the 2016 election. However, DHS and the FBI have confirmed -- and I'm going to come back to this repeatedly -- only two intrusions into the voter registration databases, in both Arizona and Illinois, even though no data was modified or deleted in those two states.
At the same time, we've seen published reports that literally dozens -- I've seen one published report that actually said 39 states -- were potentially attacked.
Certainly is good news that the attempts in 2016 did not change the results of that election. But the bad news is this will not be their last attempt. And I'm deeply concerned about the danger posed by future interference in our elections and attempts by Russian to undermine confidence in our whole electoral system.
We saw Russian -- we saw recently -- and this was just not happening here, obviously -- we saw recently Russian attempts to interfere in the elections in France. And I thank the chairman that next week we'll be having a hearing on some of these Russian efforts in Europe.
We can be sure that Russian hackers and trolls will continue to refine their tactics in the future -- future,

especially if there's no penalty for these malicious attacks.

That's again, one reason I think that the Senate voted so overwhelmingly last week, and I thank all my colleagues for that 97-2 vote to strengthen our sanctions on Russia. I hope that that action sends a strong message to Mr. Putin that there will be a heavy price to pay for attacks against the fundamental core of our democratic system.

Make no mistake, it's likely that we'll see more of these attacks not just in America but against our partners. I heard this morning coming on the radio that the Russians are already actively engaged in the German election cycle, which takes place this fall.

Now, some might say, "Well, why -- why the urgency?"

I can assure you, you know, we have elections in 2018, but in my home state of Virginia, we have statewide elections this year. So this needs a sense of urgency.

The American electoral election process, the machinery, the Election Day manpower, the actual counting and reporting primarily is a local and state responsibility. And in many states, including my own, we have a very decentralized approach, which can be both a strength and a weakness.

WARNER: In Virginia, for instance, decentralization helps deter large-scale hacking or manipulation, because our system is so diffuse. But Virginia localities use more than a dozen different types of voting machines, none of which are connected to the internet while in use, but we have a number of machine-read -- machine -- reader (ph) machines, so that they -- the tabulations actually could be broken into on an individual machine basis.

All this makes large cyber-attacks on electoral system, because of the diffusion, more difficult. But it also makes maintaining consistent, coordinated cyber defenses more challenging as well.

Furthermore, states may be vulnerable when it comes to the defense of voter registration and voter history databases. That's why I strongly believe that that the threat requires us to harden our cyber defenses and to thoroughly educate the American public about the danger.

Yesterday, I wrote to the secretary of homeland security. I urged DHS to work closely with state and local election officials to disclose publicly -- and I emphasize publicly -- which states were targeted. Not to embarrass any states, but how can we put the American public on notice when we've only revealed two states, yet we have public reports that there are literally dozens? That makes absolutely no sense.

I know it is the position of DHS that since the states were victims, it is their responsibility. But I cannot believe that this was an attack on physical infrastructure in a variety of states, there wouldn't be a more coordinated response.

We are not making our country safer if we don't make sure that all Americans realize the breadth and the extent of what the Russians did in 2016, and, frankly, if we don't get our act together, what they will do in an -- a even more dramatic form in 2018 and 2020.

And candidly, the idea of this kind of bureaucratic, "Well, it's not my responsibility, not my job," I don't believe is an acceptable decision.

So, I'm going to hope from our witnesses, particularly our DHS -- DHS witnesses, that we hear a plan on how we can get more information into the bloodstream, how we can make sure that we have better best practices, so that all states are doing what's needed.

I'm not urging or suggesting that in any way the federal government intervenes in what is a local and state responsibility. But to not put all Americans on notice, not -- and to have the number of states that were hacked into or attempt to be hacked into still kept secret is -- is just crazy in my mind.

So, my hope is that we will get some answers. I -- I do want to thank the fact that in January, DHS did designate the nation's electoral infrastructure as critical infrastructure. That's important. But if we call it critical infrastructure but then don't tell the public how many states were attacked or potentially how many could be attacked in the next cycle, I don't think we get to where we need to be.

So, we're going to have -- see more of this. This is the new normal. I appreciate the chairman for holding this

hearing. And I'm going to look forward very much to getting my questions answered.
Thank you.
BURR: Thank you, Vice Chairman.
With that, Dr. Liles, I understand you're going to go first. The floor is yours.
LILES: Chairman Burr, Ranking Member Warner and distinguished members of the committee, thank you for the invitation to be here.
My name is Sam Liles. I represent the Cyber Analysis Division of the Department of Homeland Security's Office of Intelligence and Analysis. Our mission is to produce cyber-focussed intelligence, information and analysis, represent our operational partners like the NCCIC to the intelligence community, coordinate and collaborate on I.C. products, and share intelligence and information with our customers at the lowest classification possible.
We are a team of dedicated analysts who take threats to the critical infrastructure of the United States seriously.
I'd like to begin by clarifying and characterizing the threat we observed to the election infrastructure in the 2016 election.
LILES: Prior to the election, we had no indication that adversaries or criminals were planning cyber operations against the U.S. election infrastructure that would change the outcome of the coming U.S. election.
However, throughout spring and early summer 2016, we and other -- others in the I.C. began to find indications that the Russian government was responsible for widely reported compromises and leaks of e-mails from U.S. political figures and institutions.
As awareness of these activities grew, DHS began in 2016 to receive reports of cyber-enabled scanning and probing of election- related infrastructure in some states.
From that point on, I&A began working to gather, analyze and share additional information about the threat. I&A participated in red team events, looking at all possible scenarios, collaborated and co-authored production with other intelligence community members and the National Intelligence Council. We provided direct support to the department's operational cyber center, the National Cyber Security and Communications Integration Center and worked hand-in-hand with the state and local partners to share threat information related to their networks.
By late September, we determined that internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors.
It is important to note that none of these systems were in involved in vote tallying. Our understanding of that targeting, augmented by further classified reporting is that's still consistent with the scale and scope.
This activity is best characterized as hackers attempting to use commonly available cyber tools to exploit known system vulnerabilities. This vast majority of the -- the activity we observed was indicative of simple scanning for vulnerabilities, analogous to somebody walking down the street and looking to see if you are home.
A small number of systems were unsuccessfully exploited, as though somebody had rattled the doorknob but was unable to get in, so to speak.
Finally a small number of the networks were successfully exploited. They made it through the door. Based on activity we observed, DHS made a series of assessments. We started out with, we had no indication prior to the election that adversaries were planning cyber operations against election infrastructure that would change the outcome of the 2016 election. We also assessed that multiple checks and redundancies in U.S. election infrastructures, including diversity of systems, non-internet- connected voting machines, pre-election testing and processes for media, campaign and election officials to check, audit and validate the results -- all these made it likely that cyber manipulation of the U.S. election systems intended to change the outcome of the national election would be detected.
We also finally assessed that the types of systems Russian actors targeted or compromised were not involved in vote tallying.
While we continue to evaluate any and all new available information, DHS has not altered any of these prior assessments. Having characterized the threat as we observed it, I'll stop there to allow my NPPD colleague

Jeanette Manfra to talk about more about DHS is working with election systems to add security and resiliency. I look forward to answering your questions.

BURR: Thank you.

Ms. Manfra?

MANFRA: Thank you, sir.

Chairman Burr, Vice Chairman Warner, members of this committee, thank you for today's opportunity to represent the men and women that serve in the Department of Homeland Security.

Today I'm here to discuss the department's mission to reduce and eliminate threats to the nation's critical physical and cyber infrastructure, specifically as it relates to our election.

Our nation's cyber infrastructure is under constant attack. In 2016, we saw cyber operations directed against U.S. election infrastructure and political entities. As awareness of these activities grew, DHS and its partners provided actionable information and capabilities to help -- help election officials identify and mitigate vulnerabilities on their networks.

MANFRA: Actionable information led to detection of potentially malicious activity affecting internet-connected election-related networks, potentially targeted by Russian cyber actors in multiple states. When we became aware of detected activity, we worked with the affected entity to understand if a successful intrusion had in fact occurred.

Many of these detections represented potentially malicious vulnerability scanning activity, not successful intrusion. This activity, in partnership with these potential victims and targets, enhanced our situational awareness of the threat and further informed our engagement with state and local election officials across the country.

Given the vital role that elections have in a free and democratic society, on January 26 of this year, the former secretary of homeland security established election infrastructure as a critical infrastructure sub-sector. As such, DHS is leading federal efforts to partner with state and local election officials, as well as private sector vendors, to formalize the prioritization of voluntary security- related assistance, and to ensure that we have the communications channels and protocols, as Senator Warner discussed, to ensure that election officials receive information in a timely manner and that we understand how to jointly respond to incidents.

Election infrastructure now receives cybersecurity and infrastructure protection assistance similar to what is provided to other critical infrastructure, such as financial institutions and electric utilities. Our election system is run by state and local governments in thousands of jurisdictions across the country. Importantly, state and local officials have already been working individually and collectively to reduce risks and ensure the integrity of their elections. As threat actors become increasingly sophisticated, DHS stands in partnership to support their efforts.

Safeguarding and securing cyberspace is a core mission at DHS. Through out National Cybersecurity and Communications Center, or NCCC, DHS assists state and local customers such as election officials as part of our daily operations. Such assistance is completely voluntary. It does not entail regulation or federal oversight. Our role is limited to support.

In this role, we offer three types of assistance: assessments, information and incident response. For the most part, DHS has offered two kinds of assistance to state and local officials: first, the cyber hygiene service for internet facing systems provides a recurring report identifying vulnerabilities and mitigation recommendations; second, our cybersecurity experts can go on-site to conduct risk and vulnerability assessments and provide recommendations to the owners of those systems for how best to reduce the risk to their networks.

DHS continues to share actionable information on cyber threats and incidents through multiple means. For example, we publish best practices for securing voter registration databases and addressing potential threats to election systems. We share cyber-threat indicators, another analysis that network defenders can use to secure their systems.

We partner with the multistate Information Sharing and Analysis Center to provide threat and vulnerability

information to state and local officials. This organization is partially grant-funded by DHS and has representatives that sit on our NCCC floor and can interact with our analysts and operators on a 24/7 basis. They can also receive information through our field-based personnel stationed throughout the country and in partnership with the FBI.

Finally, we provide incident response assistance at request to help state and local officials identify and remediate any possible cyber incident. In the case of an attempted compromise affecting election infrastructure, we will share that technical information with other states to assist their ability to defend their own systems from similar malicious activity.

Moving forward, we must recognize that the nature of risk facing our election infrastructure will continue to evolve. With the establishment of an election infrastructure sub-sector, DHS is working with stakeholders to establish these appropriate coordinating councils and our mechanisms to engage with them. These will formalize our mechanisms for collaboration and ensures long-term sustainability of this partnership. We will lead the federal effort to support election officials with security and resilience efforts.

MANFRA: Before closing, I want to reiterate that we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient. It is diverse, subject to local control and has many checks and balances built in. As the risk environment evolves, the department will continue to support state and local partners by providing information and offering assistance.

Thank you very much for the opportunity to testify, and I look forward to any questions.

BURR: Thank you very much.

Mr. Priestap?

PRIESTAP: Good morning.

Chairman Burr, Vice Chairman Warner, and members of the committee, thank you for the opportunity to appear before you today.

My statement for the record has been submitted. And so rather than restating it, I'd like to step back, and provide you a description of the broader threat as I see it. My understanding begins by asking one question. What does Russia want?

As you well know, during the Cold War, the Soviet Union was one of the world's two great powers. However, in the early 1990's, it collapsed and lost power, stature and much territory. In a 2005 speech, Vladimir Putin, referred to this as a major catastrophe. The Soviet Union's collapse left the U.S. as the sole super power. Since then, Russia has substantially rebuilt, but it hasn't been able to fully regain its former status or its former territory. The U.S. is too strong and has too many alliances for Russia to want a military conflict with us. Therefore, hoping to regain its prior stature, Russia has decided to try to weaken us and our allies.

One of the ways Russia has sought to do this is by influence, rather than brute force. Some people refer to Russia's activity, in this regard, as information warfare, because it is information that Russia uses as a weapon. In regards to our most recent presidential election, Russia used information to try to undermine the legitimacy of our election process. Russia sought to do this in a simple manner. They collected information via computer intrusions and via their intelligence officers, and they selectively disseminated e-mails they hoped would disparage certain political figures and shed unflattering light on political processes.

They also pushed fake news and propaganda. And they used online amplifiers to spread the information to as many people as possible. One of their primary goals was to sow discord and undermine a key democratic principle, free and fair elections.

In summary, I greatly appreciate the opportunity to be here today to discuss Russia's election influence efforts. But I hope the American people will keep in mind that Russia's overall aim is to restore its relative power and prestige by eroding democratic values. In other words, its election-related activity wasn't a one-time event. Russia will continue to pose an influence threat.

I look forward to your questions. Thank you.

BURR: Thank you very much to all of our witnesses. For members, we will proceed by seniority for recognition for up to five minutes. And the chairman will tell you when you have used all your time if you proceed that far. Chair would recognize himself for five minutes.

Yes or no to all three of you. Most important question.

BURR: Do you have any evidence that the votes themselves were changed in any way in the 2016 presidential election?

Dr. Liles?

LILES: No, sir. There was no detected change in the vote.

BURR: Ms. Manfra?

MANFRA: No, sir.

BURR: Mr. Priestap?

PRIESTAP: No, sir.

BURR: Bill, to you. This adversary is determined. They're aggressive and they're getting more sophisticated by the day. The diversity of our election system is a strength, but the intrusions in the state systems also show that Moscow is willing to put considerable resources towards an unclear result.

In 2016, we saw voter data stolen. How could Moscow potentially use that data?

PRIESTAP: They could use the data in a variety of ways. Unfortunately in this setting, I can't go into all of them. I think -- first of all, I think they took the data to understand what it consisted of; what's there, so that they can effect better understand and plan accordingly.

And when I say "plan accordingly," plan accordingly in regards to possibly impacting future elections and/or targeting of particular individuals, but also by knowing what's there and studying it. They can determine is it something they can manipulate or not, possibly, going forward. And there's a couple of other things that wouldn't be appropriate in this setting as well.

BURR: To any of you, you've heard the vice chairman talk about the frustration of publicly talking about how many states. Can you tell the American people why you can't disclose which states and the numbers?

I'll turn to Ms. Manfra first.

MANFRA: Thank you for the question, sir. There are -- through the long history that the department has in working with the private sector and state and local on critical infrastructure and cybersecurity issues, we believe it is important to protect the confidentiality that we have and the trust that we have with that community. So when the entity is a victim of a cyber incident, we believe very strongly in protecting the information around that victim.

That being said, what we can do is take the technical information that we learn from the engagement with that victim and anonymize it so it is not identified as to what that entity or individual is. We can take all the technical information and turn that around and share that broadly with -- whether it's the affected sector or broadly across, you know, the entire country. And we have multiple mechanisms for sharing that.

We believe that this has been a very important key to our success in developing trusted relationships across all of these 16 critical infrastructure sectors.

BURR: Are we prepared today to say publicly how many states were targeted?

MANFRA: We, as of right now, we have evidence of 21 states -- election-related systems in 21 states that were targeted.

BURR: But in no case were actual vote tallies altered in any way, shape or form?

MANFRA: That is correct.

BURR: How did the -- how did the French respond to the Russian involvement in the French elections a month ago? Is that something we followed?

Bill?

PRIESTAP: Senator, from the bureau's standpoint, it's something we followed from afar. We did have

engagement with French officials, but I'm just not at liberty to go into what those consisted of.
BURR: OK, we've -- we've talked about last year. Russia's intent, their target. Let's talk about next year. Let's talk about the '17 elections in Virginia. Let's talk about the '18 elections, congressional, and -- and -- and gubernatorial elections. What are we doing to prepare ourselves with this November and next November?
Ms. Manfra?
MANFRA: Yes, sir.
As we noted, we are taking this threat very seriously. And part of that is identifying this community's critical infrastructure subsector. That's allowed us to prioritize and formalize the engagement with them.
Similar to the 2016 elections, we are identifying additional resources, prioritizing our engagement with them through information sharing products, identifying in partnership, again, with the state and local community, those communication protocols -- how do we ensure that we can declassify information quickly should we need to, and -- and get it to the individuals that need it.
We're also -- have committed to working with state and local officials on incident response playbooks. So, how do they understand where to engage with us, where do we engage with them, and how do we -- are we able to bring the entire resources of the federal government to bear in helping the state and local officials secure their election systems?
BURR: Great.
Vice Chairman?
WARNER: Thank you for the answer. At 21 -- 21 states is almost half the country. We've seen reports that were even higher. I concur with the chairman that the vote totals were not changed. But can you explain to me how we're made safer by keeping the identity of 19 of those states secret from the public? Since Arizona and Illinois have acknowledged they were -- they were attacked?
LILES: Well, sir, I'd bring it back to the earlier points you made about the future elections. One of the key pieces for us within I&A is our ability to work with our partners because of how our collection mechanisms work, it's built on a high level of trust...
(CROSSTALK) WARNER: And if this was -- if this was water systems or power systems, would it be -- would the public be safer by not knowing that their water system or power system in their respective state was attacked?
MANFRA: Sir, I can -- in -- for other sectors, we apply the same principles. When we do have a victim of an incident in the electric sector, or the water sector, we do keep the name of that entity confidential. Some of these sectors do have breach reporting requirements that -- that requires the victims...
(CROSSTALK)
WARNER: Are -- are all 21 of the states that were attacked, are they aware they were attacked?
MANFRA: All of the system owners within those states are aware of the targeting. Yes, sir.
WARNER: At the state level, you could have local registrars and other local officials that -- that there may have been an attempt to penetrate at the state level. And you may have local registrars in the respective state that would not even know that their state had been the subject of Russian activities?
MANFRA: We are currently working with state election officials to ensure communication between the local and the -- and the state...
(CROSSTALK)
WARNER: But at this moment in time, there may be a number of state, local -- state, local election officials that don't know their state were targeted in 2016. Is that right?
MANFRA: The -- the owners of the systems that were targeted do know that they were targeted...
(CROSSTALK)
WARNER: The owners may know, but because we have a decentralized system, many local elective -- I just -- I...

MANFRA: I -- I cannot...
WARNER: ...fundamentally disagree. I understand the notion of victimization.
MANFRA: Yes, sir.
WARNER: But I do not believe our country is made safer by holding this information back from the American public. I got -- I have no interest in trying to embarrass any state.
WARNER: But, you know, if -- if this -- because we -- we've seen this for too long in cyber. We've seen it in the financial industry, and others, where people simply try to sweep this under the rug, and assume they'll go along their way. When we're talking about -- I go back to Liles' initial comments.
We had no idea -- we had no ability to predict this before hand. We had 21 states that were tapped. We've got two that have come forward. While no election results were changed, we do know there were a number of states, perhaps you'll answer this. How many states did the Russians actually exfiltrate data, such as voter registration lists?
MANFRA: Prefer not to go into those details in this forum, sir. I can tell you that we're tracking 21 states that were targeted...
(CROSSTALK)
WARNER: Do the states that had their data exfiltrated by the Russians -- are they aware of that?
MANFRA: Yes, sir.
WARNER: And is there any coordinated response on how we're going to prevent this going forward?
MANFRA: Yes, sir.
WARNER: How do we make sure, if states are not willing to acknowledge that they had vulnerabilities that they were subject to attack -- again, we're in a brave new world here and I understand your position. I'm not trying to -- I'm very frustrated, but I'm not -- I -- I -- I get this notion.
But I think we need a re-examination of this policy. You know, the designation by former Secretary Johnson as critical infrastructure. What does that change in terms of how our operations are going forward? By that designation in January, I appreciated it, but what does that really mean in practical terms, in terms of assistance or information sharing?
MANFRA: What it means for -- it means three things, sir. The first is a statement that we do recognize that these systems are critical to the functioning of American life, and so that is an important statement. The second is, that it formalizes and the -- and sustains, the department's prioritization of engagement with this community. And the last is, it provides a particular protection for sharing of information, in particular, with vendors within the election community. That allows us to have conversations to discuss vulnerabilities with potential systems, that we would not have to disclose.
WARNER: I -- I talked to Secretary Kelly last week, and I hope you'll take this -- at least this Senator's message, back to him. I would like us to get more information. What I've heard today is that, there were 21 states, I appreciate that information, but within those 21 states I have no guarantee that local election officials are aware that their state system may have been attacked, number one.
Number two, we don't know how many states actually had exfiltration. And the final question is, have you seen any stoppage of the Russian activities after the election? Or are they continuing to ping and try to feel out our various election systems?
MANFRA: On the first two questions, sir, I will be happy to get back to you. I spoke to the Secretary this morning and look forward to responding to your letter. On the third question, I'll defer to the FBI.
PRIESTAP: Vice Chairman, I just can't comment on our pending investigations related to the cyber...
(CROSSTALK)
WARNER: You can't say whether the -- so, should the public take away a sense of confidence that the Russians have completely stopped, as of November of 2016, trying to interfere or tap into our electoral systems. Is that what you're saying?

PRIESTAP: That's not what I'm saying, sir. I believe the Russians will absolutely continue to try to conduct influence operations in the U.S., which will include cyber intrusions.
WARNER: Thank you, Mr. Chairman.
BURR: Thank you, Vice Chairman.
To DHS and to the Bureau, a quick question, and if you can't answer it, please go back and get us an answer. Would your agency be opposed to the chair and vice chair sending a letter to the 19 states that have not been publicly disclosed, a classified letter, asking them if they would consider publicly disclosing that they were a target of the last election?
PRIESTAP: Sir, I'd be happy to take that question back to my organization, but I would just add that the role your committee is playing in regards to highlighting the Russian' aims and activities, I think, is critically important for this country.
The Bureau is just trying to balance what -- we'll call it the messaging end of that with doing things that hopefully don't impact what we can learn through our investigations. I know it's a fine -- it's a fine balance but -- but the bottom line is you play a key role in raising awareness of that, and I thank you.
BURR: Fair -- fair -- fair concern, and if both of you would just go back and get back with us, we'll proceed from there.
Senator Risch?
RISCH: Thank you much.
So that the American people can have solid confidence in what you've done, and thank you for what you've done, could you give -- could you give the American people an idea -- if you feel the numbers are classified and that sort of thing, you don't have to go into it.
But the number of people that were involved on DHS and the FBI in this investigation -- can you give us a general idea about that? Whichever one of you want to take that question.
Ms. Manfra?
MANFRA: From a DHS perspective, we did amass quite a few resources both from our intelligence and analysis and our operations analysis. To put a number on it is -- is somewhat challenging but, you know...
(CROSSTALK)
RISCH: Would you say it was substantial?
MANFRA: It was a substantial level of effort.
RISCH: You -- you're confident that you got where you wanted to go when you set out to -- to make this investigation?
MANFRA: Yes, sir. One of our key priorities was developing relationships with that community and getting information out, whether it was to specific victims or broader indicators, that we could share.
We accomplished that. We held multiple sessions. We sent over 800 indicators to the community and so we do believe that -- that we accomplished that. We don't want to let that down at all. We want to continue that level of effort and we intend to continue.
RISCH: And I'm focusing on not what you did after you got the information, but how you got the information. You're confident you got what you needed to appropriately advise everyone in this -- what was going on?
MANFRA: Yes, sir. Yes, we did.
RISCH: Mr. Priestap?
PRIESTAP: This -- the FBI considered this a very grave threat and so we dedicated substantial resources to this effort as well. RISCH: OK. Thank you. To both of you, both agencies again, everyone in this committee knows the specificity and identity of the Russian agencies involved. Are you comfortable in identifying them here today, or do you feel -- still feel that's classified?
PRIESTAP: Yeah. Other what was mentioned in the unclassified version of the intelligence community assessment, I'd rather not go into any of those details.

RISCH: And -- and -- were there any of those agencies identified, any of the Russian intelligence agencies, identified in that?
PRIESTAP: It's my understanding that GIU was identified.
RISCH: Homeland Security, same answer?
LILES: Yes, sir.
RISCH: OK. Thank you much. Let me -- let me ask this question and I come at this from a little different perspective, and I think the American people have the right to know this. From all the work that either of your agencies did, all the people involved, all the digging you did through what -- what the Russians had done and their attempts.
RISCH: Did you find any evidence, direct or circumstantial, to any degree, down to a scintilla of evidence, that any U.S. person colluded with, assisted or communicated with the Russians in their efforts?
Mr. Priestap?
PRIESTAP: And sir, I -- I just can't comment on that today. That falls under the special counsel's purview. And I have to defer to him.
RISCH: Are you aware of any such evidence?
PRIESTAP: And I'm sorry, sir, I just can't comment on that.
RISCH: Ms. -- Ms. Manfra?
MANFRA: Sorry, sir. I cannot also comment on that.
RISCH: Thank you.
Thank you, Mr. Chairman.
BURR: Senator Feinstein?
FEINSTEIN: Thanks very much, Mr. Chairman.
Candidly, I'm very disappointed by the testimony. I mean, we have learned a great deal. And the public has learned a great deal. And it seems to me we have to deal with what we've learned.
Mr. Priestap, is that correct? You have said, and I think quite pointedly, that Russia has decided to weaken us through covert influence rather than brute force. And I think that's a correct assessment, and I think you for having the courage to make it.
Here's a question. To the best of the FBI's knowledge, have they conducted covert influence in prior election campaigns in the United States? If so, when, what and how?
PRIESTAP: Yes, absolutely, they've conducted influence operations in the past. What -- what made this one different, in may regards, was of course, the degree, and then with what you can do through electronic systems today.
When they did it in the past, it was doing things like trying to put in biased or -- or half-true stories, get -- getting stories like that into the press or pamphlets that people were -- will -- would read, so on and so forth. The -- the internet is just -- has allowed Russia to do so much more today than they've even been able to do in the past.
FEINSTEIN: So, you're saying prior campaigns were essentially developed to influence one campaign above another, to denigrate a candidate if she was elected and to support another candidate subtly?
PRIESTAP: Yeah, I -- I'm saying that Russia, for years, has conducted influence operations targeting our elections, yes.
FEINSTEIN: Equal to this one?
PRIESTAP: Not equal to this one. No, ma'am.
FEINSTEIN: OK, here we go. What made this one different?
PRIESTAP: Again, I -- I think the -- the scale -- the scale and the aggressiveness of the effort, in my opinion, made this one different. And again, it's -- it's because of the electronic infrastructure, the internet, what have you, today that -- it allowed Russia to do things that in the past they weren't able to do.
FEINSTEIN: Would you say that this effort was tailored to achieve certain goals?

PRIESTAP: Absolutely.
FEINSTEIN: And what would those goals have been?
PRIESTAP: I think the primary goal in my mind was to sow discord and to try to delegitimize our free and fair election process. I also think another of their goals, which the entire United States intelligence community stands behind, was to denigrate Secretary Clinton and to try to help then -- current President, Trump.
FEINSTEIN: Have they done this on -- in prior elections in which they've been involved?
PRIESTAP: Have they...
(CROSSTALK)
FEINSTEIN: Denigrated a specific candidate and or tried to help another candidate?
PRIESTAP: Yes, ma'am, they have.
FEINSTEIN: And which elections were those?
PRIESTAP: Oh -- I'm sorry, I know there -- I -- I'm sorry, I can't think of an example off the top of my head, but even though -- all the way through the Cold War, up to our most recent election -- in my opinion, they have tried to influence all of our elections since then, and this is a common practice.
FEINSTEIN: Have they ever targeted what is admitted here today to be 21 states?
PRIESTAP: If they have, I am not aware of that. That's a -- that scale is different than what I'm aware of what they tried to do in the past. So again, the scale and aggressiveness here, separates this from their previous activity.
FEINSTEIN: Has the FBI looked at how those states were targeted?
PRIESTAP: Absolutely, ma'am.
FEINSTEIN: And what is your finding?
PRIESTAP: We have a number of investigations open in regards to that. In this setting -- I guess, because they're all still pending investigations, I'd rather not go into those details. The other thing I'd ask you to keep in mind is that we continue to learn things. So, there was some activity we were looking at prior to the election. It's not like when the election was finished our investigation stopped. So as we learn more, we share more.
FEINSTEIN: Do you know if it's the intent of the FBI to make this information public at some point?
PRIESTAP: I -- I think this gets back to an -- an issue the vice-chairman raised, and I -- I guess I want to be clear on my position on it. I think it is critically important to raise awareness about Russia's aims to undermine our democracy, and then their tradecraft and how they do it.
My organization -- part of understanding that tradecraft is -- is conducting our investigations where we learn more and more about tradecraft. So we try to balance, what do we need to provide to partners so they can best protect themselves, versus not interrupting our investigations if the information were to made -- be made public.
FEINSTEIN: Thank you very much. PRIESTAP: A balancing act.
FEINSTEIN: My time is up. Thank you.
BURR: Thanks, Senator Feinstein.
The Vice-Chairman and I have already decided that we're going to invite the bureau in for a classified briefing to update all members on the open investigations, and any that we see that might warrant, on their minds, an opening of a -- a new investigation.
In addition, let me remind members that one of the -- one of the mandates of -- of our investigation is that we will, at the end of this, work with bureau and other appropriate agencies to make a public report in as graded public detail as we can, our findings on Russia's involvement in our election.
So, it is the intent of the chair, at least, to make sure that as much as we can declassify, it's done and the public gets a -- a true understanding when we put out a final report.
Senator Rubio?
RUBIO: Thank you, Mr. Chairman.
And that's -- that's critically important. I think the most important thing we're going to do in this report is tell the

American people how this happened, so we're prepared for the next time. And what -- it begins, I think, by outlining what their goals were, what they tried to do, in this regard.

And we know what they tried to do, because they've done it in other countries around the world for an extensive period of time. The first is, undermine the credibility of the electoral process. To be able to say, that's not a real democracy. It's filled with all kinds of problems. The second is, to undermine the credibility of our leaders, including the person who may win.

They want that person to go into office hobbled by scandal and all sorts of questions about them. And the third, ideally, in their minds, I imagine, is to be able to control the outcome in some specific instances. If they think they could, either through public messaging, or even in a worst case scenario by actually being able to manipulate the vote -- which I know has now been repeatedly testified did not happen here.

RUBIO: And, by the way, these are not mutually exclusive. You can do all three, you can only take one. They all work in conjunction. I think you can argue that they have achieved quite a bit, if you think about the amount of time that we have been consumed in this country on this important topic and the political fissures that it's developed.

And the way I always kind of point to it -- and if anyone disagrees I want you to tell me this -- but, you know, we have something in American politics. It's legitimate; both sides do it. It's called opposition research. You find out about your opponent. Hopefully it's embarrassing or disqualifying information if you're the opposition research person. You package it. You leak it to a media outlet. They report it. You run ads on it.

Now imagine being able to do that with the power of a nation state, illegally acquiring things like e-mails and being able to weaponize by leaking -- leaking it to somebody who will post that and create all sorts of noise. I think that's certainly one of the capabilities. The other is just straight-out misinformation, right? The ability to find a site that looks like a real news place, have them run a story that isn't true, have your trolls begin to click on that story. It rises on Facebook as a trending topic. People start to read it. By the time they figure out it isn't true, a lot of people think it is.

I remember seeing one in early fall that President Obama had outlawed the Pledge of Allegiance, and I had people texting me about it. And I knew that wasn't true, but my point is that we have people texting about it, asking if it was. It just tells you -- and I don't know if that was part of that effort, or it was just somebody with too much time on their hands.

And then the third, of course, is the access to our voting systems, and obviously people talk about effecting the tallies. But just think about this -- even the news that a hacker from a foreign government could have potentially gotten into the computer system is enough to create the specter of a losing candidate arguing, the election was rigged. The election was rigged.

And -- and because most Americans, including myself, don't fully understand all the technology that's around voting systems per se. You give that "election is rigged" kind of narrative to a troll and a fake news site, and that stuff starts to spread. And before you know it, you have the specter of a political leader in America being sworn in under the cloud of whether or not the election was stolen because vote tallies were actually changed.

So I don't know why they were probing these different systems, because obviously a lot of the information they were looking at was publicly available. You can buy it -- voter roles. Campaigns do it all the time. But I would speculate that one of the reasons potentially is because, they wanted these stories to be out there. That someone had pinged into these systems creating a specter of being able to argue, at some point, that the election was invalid because hackers had touched election systems in key states.

And that is why I really, truly believe, Mr. Chairman, it is so important that, to the extent possible, that part of it, the systems part, as much of it be available to the public as possible. Because the only way to combat misinformation is with truth and with facts, and explain to people, and I know some of it is proprietary. I know some of it we weren't trying to protect methods and so forth, but it is really critical that people have confidence that when they go vote that vote is going to count and someone's not going to come in electronically and

change it.
And I think they're -- I -- I just really hope we err on the side of disclosure about our systems so that people have full confidence that when they go vote.
Because I can tell you, I was on the ballot in November, and I remember people asking me repeatedly, is my vote going to count? I was almost afraid people wouldn't vote because they thought their vote wouldn't count.
So I just hope as we move forward -- I know that's not your decisions to make in terms of declassifications and the like -- but it is really, really, really important that Americans understand how our voting systems work, what happened, what didn't and that -- be able to communicate that in realtime in the midst of an election.
So that if in 2018 these reports start to emerge about our voting systems being pinged again, people aren't -- we can put out enough information in October and early November so people don't have doubts. And I know that's not your decisions to make, but I just really hope that's part of -- of what we push on here, because I think it's critical for our future.
BURR: Senator Wyden.
WYDEN: Thank you, Mr. Chairman.
Let me say to the three of you, and I say it respectfully, that on the big issue, which is which states were affected by Russian hacking in 2016, the American people don't seem to be getting more information than what they already had before they showed up. We want to be sensitive to security concerns, but that question has to be answered sooner rather than later. I want to send that message in the strongest possible way. We obviously need to know about vulnerabilities, so that we can find solutions, and we need better cybersecurity to protect elections from being hacked in the first place. And that means solutions like Oregon's vote-by-mail system, that has a strong paper trail, error-gapped (ph) computers and enough time to fix the problems if they pop up.
But now to my question: You all mentioned the January intelligence assessment, saying that the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying. Your prepared system -- your prepared testimony today makes another point that I think that is important. You say it is likely that cyber-manipulation of U.S. election systems intended to change the outcome of a national election would be detected. So, that is different what we have heard thus far.
So I have two questions for you, Ms. Manfra, and you, Dr. Liles: What level of confidence does the department have in its assessment that 2016 vote tallying was not targeted or compromised? And second, does that assessment apply to state and local elections?
LILES: Thank you, sir, for the question.
So, the level of effort and scale acquired to change the outcome of a national election would make it nearly impossible to avoid detection. This assessment's based on the diversity of systems, the need for physical access to compromise voting machines themselves, the security of pre-election testing employed by the state and local officials. There's a level -- a number of standards and security protocols that are put in place. There's a -- addition, the vast majority of localities engage in logic and accuracy testing, which work to insure voting machines are operating and tabulating as expected.
Before, during, and after the election, there has been an immense amount of media applied to this, which also brings in the idea of people actually watching in and making sure that the election results represent what they see. And plus there's just this statistical anomalies that would be detected, so we have a very high confidence in our assessments.
WYDEN: What about state and local elections? Do you have the same level of confidence?
LILES: So, from the standpoint of a nation-state actor operating against a state and local election system, we would have the same -- for an Internet-connected system, we would have the same level of confidence.
WYDEN: Ms. Manfra?
MANFRA: Yes, sir.
And I think this also gets to Senator Rubio's point about the difficulty in the general public understanding the

variety of systems that are used in our election process.
MANFRA: And so, we broke our level of engagement and concern down a couple of different areas. The voter registration systems, which are often -- can -- usually connected to the internet. We also were looking at the voting machines themselves, which, by best practice and by the voluntary voting standards and guidelines that the Department of Commerce works with the Election Assistance Commission on, is, by best practice -- those are not connected to the internet.
WYDEN: So can Homeland Security assure the public that the Department would be able to detect an attempted attack on vote tallying?
MANFRA: What I would suggest, sir, is that the ability, as has been demonstrated by security researchers, to access remotely, a voting machine to manipulate that vote, and then to be able to scale that across multiple different voting machines made by different vendors, would be virtually impossible to occur in an undetected way within our current election system.
WYDEN: Has the department conducted any kind of post-election forensics on the voting machines that were used in 2016?
MANFRA: We are currently engaged with many vendors of those systems to look into conducting some joint forensics with them. The vendor community is very interested in engaging with us. We have not conducted...
(CROSSTALK)
WYDEN: So there's no -- there's been no analysis yet?
MANFRA: We have not -- our department has not conducted forensics on specific voting machines.
WYDEN: Do you believe it's important to do that? In terms of being able to reassure Americans that there was no attack on vote tallying?
MANFRA: Sir, I would say that we do currently have voluntary standards in place that vendors are enabled -- and in approximately 35 states, actually require, some level of certification of those voting machines that they are complying with those standards. We would absolutely be interested in working with vendors to conduct that level of analysis.
WYDEN: Let me ask one last question. Obviously, the integrity of elections depends on a lot of people. State and local election officers, equipment vendors, third party contractors.
Are you all, at Homeland Security and the FBI, confident that the federal government has now identified all of the potential government and private sector targets?
MANFRA: Yes, sir. I'm confident that we've identified the potential targets.
WYDEN: OK.
Thank you, Mr. Chairman.
BURR: Senator Collins?
COLLINS: Mr. Priestap, let me start by saying that it's a great pleasure to see you here again. I remember back in 2003, you were detailed to the Homeland Security Committee when I was the chairman and how helpful you were in our drafting the Intelligence Reform and Terrorism Prevention Act. So, thank you for your continued public service.
You testified this morning and answered the question of, what does Russia want? And you said that the Russians want to undermine the legitimacy of our elections and sow the seeds of doubt among the American public.
Despite the exposure and the publicity given to the Russian's efforts in this regard, do you have any doubt at all that the Russians will continue their activities in subsequent elections?
PRIESTAP: I have no doubt. I just can't -- I just don't know the scale on aggressiveness, whether they'll repeat that, if it'll be less or if it'll be more. But I have no doubt they will continue.
COLLINS: Is there any evidence that the Russians have implanted malware or backdoors or other computer techniques to allow them the easier access next time to our election systems?

PRIESTAP: I'm sorry, Senator. I just can't comment on that because of our impending investigations.
COLLINS: Secretary Manfra, the secretaries of state who are responsible for the election systems have a pretty blistering attack on the Department of Homeland Security, in the testimonies that will be given later this morning. And I want to read you part of that and have you respond.
They say, yet nearly six months after the designation -- and they mean the designation of election systems as critical infrastructure -- and in spite of comments by DHS, that they are rushing to establish election protections. No secretary of state is currently authorized to receive classified threat information that would help them to protect their election systems. Why not?
MANFRA: Thank you, ma'am, for that question. I would note that this community -- the secretaries of state, and for those states where they have a state election director, is not one that the department has historically engaged with. And what we have done in the process of building the trust and learning about how they do their work and how we can assist, we have identified the need to provide clearances to that community. And so we have committed to them to work through that process between our department and the FBI.
COLLINS: Let me ask you about your own agency, which is the agency that focuses on critical infrastructure, including our election systems. Now, NPPD is not an official element of the intelligence community that would have routine access to especially sensitive classified information.
So how do you know with any certainty whether you and others in the agency are read into all the relevant classified information that may exist regarding foreign threats to our critical infrastructure, including our election system?
MANFRA: Yes, ma'am. I would say, despite the fact that we're not a part of the intelligence community -- and our focus is on network defense and operations, in partnership with the critical infrastructure and the federal government -- we feel very confident that with the partnership with our own intelligence and analysis division, that serves as an advocate for us within the intelligence community, as well as our direct relationships with many of those individuals in organizations such as the FBI, NSA and others, that we receive information quickly. And when we ask to declassify that, there are responses, and we work through our partners at the intelligence analysis office to ensure that that happens quickly. So is there room for improvement? Absolutely, of course, but we have the full commitment of the intelligence community to support us and get us the information that we need and our stakeholders need.
COLLINS: And, finally, how many states have implemented all the best practices recommended in the document developed by DHS regarding the protection of election systems?
MANFRA: Ma'am, I'd have to get back to you on a specific number of states. I don't have them.
COLLINS: Do you think most states have?
MANFRA: In our informal engagement, many of them noted that they had already adopted some of these and to the extent that they weren't -- they were incorporating them.
COLLINS: I would ask for a response for the record.
MANFRA: Yes, ma'am.
COLLINS: That's a really important point.
BURR: Senator Heinrich?
HEINRICH: Mr. Priestap, I want to thank you for just how seriously you've taken this and how you've answered the questions this morning in your testimony. I think you hit the nail on the head when you said we need to step back and ask the fundamental question, what do the Russians want?
And by outlining that they want to undermine legitimacy in our system, that they want to sow discord, that they want to undermine our free and fair elections, we really have a better lens with which to understand the -- the specifics of what happened in 2016. In -- in your view, were the Russians successful at reaching their goals in their activities in our 2016 elections?
PRIESTAP: I don't know for certain whether the Russians would consider themselves successful. In many

 18-F-1517//1229 ProQuest

ways, they -- they might argue that because of the time and energy we're spending on this topic, maybe it's distracting us from other things. But, on the other hand, exactly what this committee is doing as far as raising awareness of their activities, their aims, for the American people, to me they've done -- in my opinion, they've done the American public a service in that regard. And so, I guess I don't know but could argue either way.
HEINRICH: Yes. I -- I think the -- the jury's certainly out for the future, but when you look at the amount of discord that was sown and the impact on 2016, I hope that the outcome of what we're doing here is to make sure that in 2018, and in 2020, and 2022, that by no metric will they have been successful.
Mr. Priestap, you stated, very correctly, that one of their primary goals was to delegitimize our democracy. Are -- are you familiar with the term unwitting agent?
PRIESTAP: Yes, I am.
HEINRICH: Can you kind of summarize what that is for us?
PRIESTAP: In an intelligence context, it would be where an intelligence service is trying to advance certain names and they reach out to a variety of people, some of which they might try to convince to do certain things. And the -- the people, person or persons they contact might actually carry those out, but for different reasons than the intelligence service that actually wanted them to carry them out. In other words, they do it unwittingly.
HEINRICH: By effectively reinforcing the Russian narrative and -- and publicly saying that our system is rigged, did then candidate Trump -- now President Trump, become, what intelligence officials call, an unwitting agent?
PRIESTAP: I -- I can't give you a comment on that.
HEINRICH: I -- I don't blame you for not answering that question. We've got about a minute 46 left. Can you talk about the relationship between the election penetration that we saw and the coincident Russian use of, what Senator Rubio very aptly described, of trolls, of bots, of social media, all designed to manipulate the American media cycle and how those two things fit together?
PRIESTAP: I'm sorry. To clarify, fit together the intrusions with the...
(CROSSTALK)
HEINRICH: What's the relationship between what they were doing in our elections, from a technical point of view, and what they were seeking to do in our media cycle, by using trolls, and bots and manipulation to the media cycles.
PRIESTAP: The -- the -- I guess the best way I can describe it is that this was a, my opinion, a well planned, well coordinated, multi-faceted attack on -- on our election process and democracy. And, while that might sound complicated, it was actually really straight forward. They want to collect intelligence from a variety of sources, human and cyber means.
They want to evaluate that intelligence, and then they want to selectively -- they might selectively disseminate some of it. They might use others for more strategic discussions, but at the end of the day, it's all about collecting intelligence that would give them some type of advantage over the United States and/or attempt to influence things. And then, coordinated -- well coordinated, well funded, diverse ways to disseminate things to hopefully influence American opinion.
HEINRICH: This is a very sophisticated, highly resourced...
(CROSSTALK)
PRIESTAP: Absolutely.
HEINRICH: Thank you.
BURR: Senator Blunt?
BLUNT: Thank you. Thank you, Chairman.
Let's talk a little bit about once -- let's start with a comment that DHS made in it's written comment which -- which says, in excess, that the systems Russian actors targeted or compromised were not involved in vote tallying. Now is that because the vote tallying systems are a whole lot harder to get into than the voter registration systems?

MANFRA: I can't make a statement as to why different systems were targeted. What we can assess that is that those vote tallying systems, whether it was the machines or a kiosk that a voter uses at the polling station, or the systems that are used to tally votes, were very difficult to access, and particularly, to access them remotely. And -- and then given the level of observation of -- for vote tallying at every level of the process that adds into, you know, that we would have identified issues there and there were no identified issues. So those two are... (CROSSTALK)

BLUNT: OK. I -- I would think that if you could get into the vote tallying system, and you did want to impact the outcome of an election, obviously, the vote tallying system is the place to do that. And I would also suggest that all of your efforts -- most -- a lot of your efforts should be to continue to do whatever DHS thinks they need to advise. I don't think we should centralize this system to give advice to state and local election officials to be sure that that that vote tallying system is protected at a level above other systems.

You know, the voter registration system is public information. It is generally accessible in lots of ways. It's not nearly as protected, for that reason. You have lots of them put from lots of sources into that system. And I think, Ms. Manfra, you made the point that you said that in a -- the best practice would be to not have the vote tallying system connected in any unnecessary way to the internet. Is that right?

MANFRA: Both the kiosks themselves and vote tallying systems, to not connect them to the internet and to also have, ideally, paper auditing trails as well.

BLUNT: Well, I certainly agree with that. The paper trail is significant and -- and I think more prevalent as people are looking at new systems. But also, I think any kind of third party monitoring, the third -- the first two parties would be the voter and the counting system, just creates another way into the system. So, my advice would be that DHS doesn't want to be in a situation where somehow you're connected to all the voting systems of the country.

And Mr. Liles, I think you said the diversity of our voting system is a great strength of the system. Do you want to comment on that any more?

LILES: Yes, sir. When we were setting it as part of our red teaming activities, we looked at the diversity of the voting system as actually a great strength. And the fact that there were not connected in any one kind of centralized way. So we evaluated that as -- when we were looking at the risk assessment with OCIA, the Office of Cyber Intelligence Analysis -- Infrastructure Analysis, we looked at that as one of the great strengths and our experts at DIC we worked with also said the same thing.

BLUNT: Well, I would hope you'd continue to think about that as one of the great strengths, as you look at this critical infrastructure, because every -- every avenue for federal monitoring is also just one more -- one more avenue for somebody else to figure out how to get into that system.

And again, the voter registration system dramatically different in what it does. All public information accessible, printed out, given to people to use, though you are careful of what information you give and what you don't. But almost all election officials that have this system now, have some way to share that with the public, as a system.

There is no reason to share the security of the vote counting system with the public, or to have it available or accessible. And I would hope that the DHS, or nobody else, decides that you're going to save this system by having more avenues -- more avenues into the system.

MANFRA: Absolutely not, sir. We're fully supportive of the voluntary standards process, and we are engaging with that process with our experts and we continue, again, with the voluntary partnership with the state and local. And we intend to continue that.

BLUNT: Thank you. Thank you, Mr. Chairman.

BURR: Senator King?

KING: Thank you, Mr. Chairman.

Starting with a couple of short questions, Mr. Priestap.

Number one, you've stated this was a very grave threat, that Russia -- the attempts to probe and upset our local election systems. Any doubt it was the Russians?
PRIESTAP: No, sir.
KING: Any doubt that they'll be back?
PRIESTAP: No, sir.
KING: To our DHS witnesses, have the 21 states that you've mentioned, that we know where we had this happen, been notified officially?
MANFRA: Sir, the owners of the systems within those 21 states have been notified.
KING: How about the election officials in those states?
MANFRA: We are working to ensure that election officials as well understand. I'll have to get back to you on whether all 21 states...
(CROSSTALK)
KING: Have you had a conference of all state election officials, secretaries of state here in Washington on this issue?
MANFRA: I have had at least two teleconferences, and in-person conferences -- we will be engaging with them in July, I believe.
KING: Well, I would urge you to put some urgency on this. We've got another election coming in 18 months and if we're talking about systems and registration rules, the time is going by. So, I believe, this is -- as we've already heard characterized, is a very grave threat. It's going to be back and shame on us if we're not prepared.
MANFRA: Yes, sir. We have biweekly -- every other week, we hold a teleconference with all relevant election officials, the national associations that represent those individuals have nominated bipartisan individuals to engage with us on a regular basis.
This is of the utmost urgency for the department and this government to ensure that we have better protections going forward. But the community -- the election community is similarly committed and has been so for years.
KING: And just to be clear, nobody's talking about a federal takeover of local election systems or the federal rules. What we're talking about is technical assistance in information and perhaps some funding, at some point.
MANFRA: Sir, this is similar to our engagement with all critical infrastructure sectors, whether it's the electrical sector, the nuclear sector, the financial sector, is completely voluntary, and it is about this department providing information, both to potential victims, but to all network defenders, to ensure that they have access to what we have access to and can better defend themselves.
KING: Thank you.
Mr. Liles, I'll take issue with something that you said -- that we have a national election and it was just too large, too diverse, to really crack. We don't have a national election. What we have are 50 state elections. And each election in the states can depend upon a certain number of counties.
There are probably 500 people within the sound of my voice who could tell you which ten counties in the United States will determine the next presidential election. And so you really -- a sophisticated actor could hack a presidential election, simply by focusing on particular counties. Senator Rubio, I'm sure, remembers Dade County in the year 2000 and the significance that had to determining who the next president of the United States was.
So, I don't think it works to just say, oh, it's a big system and the very diversity will protect us because it really is county by county, city by city, state by state and a sophisticated actor, which the Russians are, could easily determine where to direct their attack. So I don't want to rely on the diversity.
Second -- a separate point is, what do we recommend? And we've talked about paper backups. The Dutch just had an election where they just decided to make it all paper and count the ballots by hand, for this very reason. So what would you tell my elections clerk in Brunswick, Maine, Ms. Manfra, would be the top three things he or she should think about in protecting themselves in this situation?

MANFRA: Sir, I would say, to first, as previous senators mentioned, prioritize the security of your voting machines and the vote tallying system, ensure that they are not connected to the internet -- even if that is enabled on those particular devices.

Second, ensure that you have an auditing process in place where you can identify anomalies throughout the process, educate polling workers to look for suspicious activity, for example.

KING: But does -- doesn't auditing mean a paper trail, a paper backup?

MANFRA: Yes, sir. I would recommend a paper backup.

KING: And one of the worrisome things, again, on the issue of the national, we talk about how diverse it is, but aren't we seeing a consolidation in terms of the vendors who are producing these machines? MANFRA: Yes, sir. It is my understanding that we are seeing some consolidation in the vendor community. Again, many of them are committed and have engaged on the voluntary voting standards and guidelines, which partly include security.

We will be updating those security guidelines in 2018, and yes, while there is some concern about consolidation, we do look forward to engaging with them, and as of now, they are a very engaged community.

KING: I think this aspect of this question that we're -- this committee is looking at is one of the most important, and frankly, one of the most daunting, because we pretty well determined that they weren't successful in changing tallies and changing votes but they weren't doing what they did, in at least 21 states, for fun.

And they are going to be back, and they're going to be back with knowledge and information that they didn't have before. So I commend you for your attention to this and certainly hope that this is treated with the absolute utmost urgency.

KING: Thank you, Mr. Chairman.

BURR: Senator Lankford?

LANKFORD: Thank you, Mr. Chairman.

Thanks to all of you for being here as well today.

So, Senator King, just as a heads up, there are some states that are like that. For 25 years the Oklahoma election system has had a paper ballot, and an optical scan and it's been a very good back-up for us. We -- we quickly count because of the optical scan, but we're able to go back and verify because of paper.

This is such a big deal and it's such an ongoing conversation that I'm actually in two simultaneous hearings today, I'm running back and forth with. In the Department of Homeland Security, and what we're dealing with with state elections, and with state systems, is also happening in the HSGAC hearing that I'm also at, including my own Oklahoma CIO that's there testifying today, on this same issue.

How we are protecting state systems, state elections and what's happening? I brought this with me today, you all are probably -- this group is very, very familiar with this e-mail. This is the famous e- mail that Billy Rinehart got, from the DNC, while he happened to be on vacation. He was out in Hawaii enjoying some quality time away from his work at the DNC, and he gets a -- an e-mail from Google, it appears, that says someone has used your password, someone just tried to sign-in to your Google account.

Sent it to him and told him someone tried to do it from the Ukraine, and recommended that he go in and change his password immediately. Which, as the New York Times reported, he groggily at 4 a.m., when he saw that e-mail was frustrated by it, went in, clicked on the link, changed his password and went back to bed.

But what he actually did, was just gave the Russian government access to the DNC, and then it took off from there. Multiple other staff members of the DNC got an e-mail that looked just like this. Now, for everyone who has a Google account, will know that really looks like a Google account warning.

It looked like the real thing when you hovered over the changed password, it showed a Google account connection, where it was going to, but it wasn't. It was going to the Russians. About 91 percent, my understanding is, about 91 percent of the hacks that come into different systems, start with a spear phish attack that looks just like this.

So let's -- let's talk about, in practical terms, for our state election folks and what happens in my state and other states. First, for you, Mr. Priestap, how does Russia identify a potential target? Because this is not just a random e-mail that came to him, this was targeted directly at him, to his address. It looked very real, because they knew who he was and where he works. So, how were the Russians that savvy to be able to track this person and how does this work in the future for an election system for a state?

PRIESTAP: So I can't go into great detail in this forum, but I'd say what intelligent services do, not just Russia there, is they're looking for vulnerabilities. That -- that would begin in the cyber sense with computer vulnerabilities. As far as targeting specific individuals, I -- I don't know all the facts surrounding that e-mail and all the e-mails were sent, but my guess is, they didn't just send it to one person. They send it -- sent it the e-mail like that to a whole variety of -- just hoping that one would click on it.

LANKFORD: Right. But how are they getting that information? Are they going to their -- their website, for instance, and gathering all the e-mails for it? I'm trying to figure out, are they tracking individuals to get more information, so they get something that looks like something they would click on?

PRIESTAP: Yes. You hit on it, but a whole variety of ways. They might get it through reviewing open source material, either online or otherwise, but they also collect a lot of information through their -- through human means.

LANKFORD: So, Ms. Manfra, let me ask you this question. When someone, at any location, clicks on a link like this, what access to information do they get typically?

MANFRA: Well, sir, it depends on -- on the system itself. I -- I imagine that's probably a frustrating response, but given the -- and I think this is important for the public to understand, is, as the -- the threat evolves they're going to continue as we educate the public, don't click on certain things. Look at, you know, make sure you know the sender, for instance before you click on it and as our defense gets better the offense is going to look for other means.

And so we look, you know, in this case, ideally, we want people to look and see what -- what is it that they're actually clicking on before they click it. Some organization to -- to say when an individual clicks on that link, they choose to not allow that to go to that destination, because they know it's suspicious or they have some mechanisms in place to put that into a container and look at it. Other organizations don't take those steps and it really depends on your risk management and the technical control that you put in place.

LANKFORD: Let me ask you a quick question. Who has primary responsibility for Federal election integrity? Which agency is the prime mover in that? Obviously, states oversee their own, but which Federal entity is working with the state to say they're the prime person -- or the prime agency to do it? MANFRA: For election cybersecurity, our -- our department, in coordination with the FBI and others, is leading the partnership with state and locals.

LANKFORD: Great. Thank you.

BURR: Senator Manchin?

MANCHIN: Thank you, Mr. Chairman.

And thank all of you for your appearance here today and your testimony. Being a former Secretary of state of the -- my great state of West Virginia, and also being a former governor, my utmost concern was voter fraud. Every time that we would have a report of a fraud, I would see the election participation decrease, the next election cycle, thinking their vote didn't count.

Is there any reason, at all, that any person that has the knowledge that you all have, or anyone that you've -- on our committee here, from the intelligence community, would give you any doubt that Russia was involved, and Russia was very much involved with the intent of doing harm to our election process, as far as the confidence level that voters would have? Do any of you have any concerns, whatsoever, any doubts, that the Russians were behind this and involved in a higher level than ever? All three of you.

PRIESTAP: No -- no doubt from the FBI's end as far as the -- as far as Russia's involvement.

MANCHIN: And you've all interacted with all the intelligence community right?
PRIESTAP: Yes, sir.
MANFRA: Similar, sir. I have no doubt.
MANCHIN : There's not an American right now that should have a reasonable doubt whatsoever that the Russians were involved? Were all 50 states notified on Russia's intentions and activities during the '20 (sic) election cycle? Had you all put an alert out? So if I'd have been secretary of state in charge of my elections in West Virginia, would you have notified me to be on the lookout?
MANFRA: Sir, I can discuss our products that we put out and I'll defer to the FBI on -- on what they put out. We did put out products, not public products, but we did put out products, primarily leveraging our multi-state information sharing analysis center, which has connections to all 50 states CIOs.
And we engaged with the Election Assistance Commission and other national associations that represent those individuals to ensure that we were able to reach, again this was a community that we had not historically engaged with, and so, we relied on those, that we did put out multiple products prior to the election.
MANCHIN: And you're really not sure if these national associations, like (ph) the secretary of states, dispersed that information, put everybody on high alert?
MANFRA: I -- I believe that they did, sir. We also held a conference call, where all 50 secretaries of state, or an election director, if the -- if the secretary of state didn't have that responsibility. In August, and September and again in October, both high level engagement and network defense products.
MANCHIN: And if I could ask this questions to whoever, maybe Mr. Priestap, what was Russia's intention, and do you think they were successful in what they desired to do, even thought they didn't alter -- as you all have said, you can see no alterations of the election results. Do you believe that it had an effect in this election outcome -- in the outcome of this 2016 election?
PRIESTAP: As far as Russia's intention, again, the broader being to undermine democracy and one of the ways they sought to do this, of course, here, was to undermine the legitimacy of our free and fair election.
MANCHIN: Do you believe they were successful in the outcome?
PRIESTAP: No, I -- the FBI doesn't look at that, as far as, did Russia achieve its aims in that regard.
MANCHIN: Let me ask this question. Are there counter actions the U.S. can take to subvert or punish the Russians for what they have done, and their intention to continue? And what's your opinion of the sanctions that we have placed on Russia?
PRIESTAP: Sure. As you know, the FBI doesn't do policy. I'm here today to provide you an overview of the threat picture, at least, as I understand and see it. But obviously the U.S. government did take action post-election in regards to making a number of Russian officials...
(CROSSTALK)
MANCHIN: Have you seen them subside, at all, any of their activities since we have taken some actions?
PRIESTAP: Subside? They have less people to carry out their activities, so it's certainly had an impact on the number of people.
MANCHIN: And finally, with the few seconds I have left, have we shared this with our allies, our European allies, who are going through election processes and have they seen the same intervention in their election process that we have seen from the Russians in ours? PRIESTAP: Sure. I can't speak for DHS, but the FBI is sharing this information with our allies, absolutely.
MANCHIN: How about DHS?
MANFRA: We are also sharing information with our allies.
MANCHIN: Are they seeing a high -- an overaggressive, high activity, from the Russians that they haven't seen at this level before, such as we did during the 2016 election?
LILES: Sir, there is immediate reporting that suggests that. We don't have direct government-to-government relationships from a DHS perspective. There is definitely immediate reporting that they're seeing an increased

activity.
MANCHIN: Thank you.
BURR: Senator Cotton?
COTTON: Thank you all for your appearance today.
Mr. Priestap, in response to Mr. Heinrich's question about whether Donald Trump had become an unwitting agent of Russia, and their efforts to sow discord and discontent about our elections, you said that you decline to answer, which is understandable.
Let's look at this from a different perspective. Since her election defeat, Hillary Clinton has blamed her loss on the Russians, Vladmir Putin, the FBI, Jim Comey, fake news, Wikileaks, Twitter, Facebook and my personal favorite, content farms in Macedonia. In her blaming her loss on these actors, has Hillary Clinton become an unwitting agent of Russian's goals in the United States?
PRIESTAP: And I'm sorry, sir, but I'd rather not comment. It's just something...
(CROSSTALK)
COTTON: I understand. I just wanted to point out that you can look at it from two different...
(CROSSTALK)
PRIESTAP: ...it's just something I haven't given any thoughts to.
COTTON: Let's turn to other matters, then. Would you advise states and localities in the conduct of their elections, or more broadly, in their government services, not to use, or not to do business with Kaspersky Labs, companies that do business with Kaspersky or companies that use Kaspersky products in their systems?
PRIESTAP: Sir, I can't really comment on that in this setting.
COTTON: Miss Manfra, would you advise them not to use Kaspersky products?
MANFRA: I also cannot comment on that in this forum, sir.
COTTON: I don't even have to ask, Dr. Liles. You're reaching for your microphone.
LILES: Yes, sir. I can't comment either.
COTTON: OK. Senator Risch says he'll answer, but I'll let him speak for himself at a later time. Mr. Priestap, we've talked a lot about Russia's intent and activities in our elections but I think it's important that the American people realize that it goes much farther than just elections and the 2016 campaign, as well.
Isn't it true that Russian cyber actors have been probing U.S. critical infrastructure for years?
PRIESTAP: Yes, sir. I can't go into specifics but they probe a lot of things of critical importance to this country.
COTTON: And as the head of counter intelligence, you write in your statement, that quote, "Russia's 2016 presidential election influence effort was its boldest, to date, in the United States" which implies there have been previous efforts. You also say that the FBI had to strengthen the intelligence community assessment because of our history investigating Russia's intelligence operations within the United States. Both of which suggest that this keeps you pretty busy in your portfolio and counterintelligence, is that right?
PRIESTAP: That's correct.
COTTON: And this is -- Russian intelligence threat is not just a cyber threat either. It also is a threat from traditional human intelligence, or what a layman might call spies, is that right?
PRIESTAP: Yes, sir.
COTTON: Do so called diplomats who work down at the Russian embassy in Washington D.C. have a requirement to notify our state department in advance if they plan to travel more than 25 miles, and give that notification 48 hours in advance?
PRIESTAP: They do.
COTTON: And the State Department's supposed to notify the FBI in advance of those travel arrangements, correct?
PRIESTAP: Yes.
COTTON: Is it true that the Russian nationals often fail to give that notification, at all, or they give it at, say, 4:55

on a Friday afternoon before a weekend trip?
PRIESTAP: I'd prefer not to go into those details here, but -- I'll leave it at that. COTTON: Does it complicate you and your agents' efforts to conduct your counterintelligence mission, to have Russian nationals wandering around the country more than 25 miles outside their duty assignment?
PRIESTAP: Sure. If that were to happen, that would absolutely complicate our efforts.
COTTON: The Secretary of Defense recently indicated, at a Armed Services Committee hearing, that Russia is in violation of something called the Open Skies Treaty, a treaty we have with Russia and other nations that allow us to overfly their territory and take pictures and they do the same here. Do we see so called Russian diplomats traveling to places that are in conjunction with open skies flights that Russia's conducting in this country?
PRIESTAP: I'm sorry, I just can't comment on that here.
COTTON: OK. Is it -- so last summer, a American diplomat in Moscow was brutally assaulted on the doorstep of our embassy in Moscow. Did we take any steps to retaliate against Russia for that assault in Moscow? Did we declare persona non grata any of their so called diplomats here in the United States?
PRIESTAP: If I recall correctly, we didn't immediately do anything in that regard.
COTTON: OK. This committee passed, unanimously, in committee last year, something that just passed as part of the (inaudible) in April a provision that would require one, the State Department to notify the FBI of any requests for Russian diplomats to travel outside their embassy and to report violations to you.
It further requires the State Department to report those violations, regularly, to this committee. What's the status of that provision, now that it's been in law for about two months? Is the State Department cooperating more fully with you?
PRIESTAP: I guess I'd rather not comment on that here. We're still working through the implementation of that.
COTTON: Well, I certainly hope they start. Thank you.
BURR: Senator Harris?
HARRIS: Thank you. Ms. Manfra, you mentioned that you notified the owners. I'm not clear on who the owners are. Are they the vendors?
MANFRA: What I meant to clarify is, in some case, it may not be the secretary of state or the state election director who owns that particular system, so in some cases it could be a locality or a vendor.
HARRIS: So is there a policy of who should be notified when you suspect that there's a threat?
MANFRA: We are working through that policy with the secretaries of state, that is one of the commitments that we made to them, as election directors, in order to ensure that they have appropriate information, while preserving the confidentiality of the victim, publicly.
HARRIS: And can you tell us which states - in which states you notified the vendor instead of notifying the secretary of state?
MANFRA: We keep the vendor information confidential as well.
HARRIS: Are there states that you notified where you did not notify the person who was elected, by the people of that state, to oversee elections?
MANFRA: I don't believe that's the case but I will get back to you with a definitive answer.
HARRIS: And how specific was the warning that you sent? What exactly is it that you notified the states or the vendors of?
MANFRA: Depending on the scenario, and the information that we had, and more generally what we do, is when we get classified information, we look to declassify as much as possible to enable...
(CROSSTALK)
HARRIS: Let's talk about the election, yeah.
MANFRA: So for this particular one, what we took was technical information that we had, that we believed was suspicious, and that was emanating from Russia, and was targeting their system, we asked them to look at their

system. We asked, and this was part of the broader dissemination, as well, we asked all states to look at their system, to indentify whether they had an intrusion, or whether they blocked it. In most cases, they blocked it.
HARRIS: Do you have a copy with you of the notification you sent to these various vendors or states?
MANFRA: I do not, ma'am, but we can get back to you.
HARRIS: OK, and will you provide this committee with a copy of the notification you sent to those states or vendors?
MANFRA: Many of them were done in person, but what I can show you is the technical information. That was also rolled up in the information that we published in December, but I can show you what we provided to the states and localities.
HARRIS: And did you notify each of them the same way? Or did you tailor the notification to each state?
MANFRA: We tailor the notification. It's a process for all victim, or potential victim, notification -- us and the FBI, so sometimes it may be an FBI field agent that goes out there, sometimes it may be a department official that goes out there.
HARRIS: OK, so in your follow-up to the committee, please provide us with, specifically, who notified each state, and then who in that state was notified, the vendor or the state election official, and also what specifically they were notified of. I have, in 2007, California worked with leading security researchers, the secretary of state at the time was Deborah Bowen, and they instituted some of the best practices, we believe, for election security. And my understanding is that it is considered a gold standard. So my question is, does DHS have the technical capability and authority to coordinate a study like that for all of the states?
MANFRA: We do have the technical capability and authority to conduct those sorts of studies, ma'am, yes.
HARRIS: Have you pursued that as a viable option to help the states do everything they can to secure their system?
MANFRA: That is one of the areas that we're considering, yes, ma'am.
HARRIS: So have you taken a look at that study that was commissioned in California, in 2007? And if not, I'd encourage that you do.
MANFRA: I have not personally, but I will read it, ma'am.
HARRIS: And I'm also concerned that the federal government does not have all the information it needs in these situations where there's been a breach. Is there any requirement that a state notify the federal government when they suspect there's been a breach?
MANFRA: No, ma'am.
HARRIS: And in terms of the American public and voters in each of these states, can you tell me is there any requirement that the state notify its residents when the state suspects there may be a breach?
MANFRA: I cannot comment. I know that multiple states have different sunshine laws, et cetera, that apply to data breaches within the state, so I couldn't make a general statement about what their requirements are at the state level.
HARRIS: And do any of you have any thoughts about whether there should be such requirements, both in terms of states reporting to the federal government, and also states reporting to their own residents and citizens about any breaches of their election system?
MANFRA: Required data breach reporting is a complicated area. We prefer, and we've had a fair amount of success with, voluntary reporting and partnerships, but we'd be happy to work with your staff in further understanding how that might apply here.
HARRIS: OK, I appreciate that. Any other thoughts, as we think about how we can improve notification and sharing of information? No. OK, thank you.
BURR: Before I move to Senator Reed, let me just say that since a number of members have questioned the agencies, especially those that are here, and the sharing with Congress of the investigation, I'll just say that the Chair and the Vice Chair were briefed at the earliest possible time, and continued to be briefed throughout the

process, and then it was opened up to all the members of the committee. I'm not sure that I had ever shared that with everybody but I just want to make sure that everybody's aware of that.

Senator Reed?

REED: Thanks very much, Mr. Chairman.

Thank you very much, ladies and gentlemen. Let's start with Mr. Priestap. Are you aware of any direction or guidance from President Trump to conduct this investigation about the Russian cruising (ph) in our elections?

PRIESTAP: Sir, I can't comment on that. It could be potentially related to things under the special councils purview.

REED: Thank you.

Ms. Manfra, in terms of home security, are you aware of any direction by the president to conduct these types of operations, or your investigations?

MANFRA: Sir, to clarify the question, direction from the president to...

(CROSSTALK)

REED: The President of the United States has directed that we, the Department of Homeland Security, and other federal agencies conduct a - the activities that you're conducting, essentially investigation, in to Russian hacking in the election.

MANFRA: I can't comment on the president's directions, specifically, but our secretary is committed to understanding what happened, ensuring that we are better protected in the future, so our activities are fully supported.

REED: He has not communicated that this is at the direction of the President of the United States?

MANFRA: No, sir.

REED: Director Liles?

LILES: Sir, this comes directly written down from the IC (ph) who has been working on this for quite a while, and so, and the secretary has completely supported it.

REED: But again, no...

(CROSSTALK)

LILES: Nothing from the president directly, sir.

REED: Thank you. I thought Senator King raised some very interesting issues, in terms of most election - national elections, as much you like to think about it, particularly from Rhode Island, are not decided in certain states, but decided even in certain cities and counties. Which raised an interesting question -- you were very assertive about that you'd be able to diagnose an intrusion that was altering voter -- votes, literally. When could you do that? Within weeks of an election, on Election Day, after Election Day?

LILES: Sir, from an IEC perspective, the way we would do that is by looking at the threats themselves that were targeting specific entities. And the other element that we would look at is, as the reporting itself was coming in, if there was any statistical anomalies we were seeing. And I'd also point out, that we're talking about internet-connected systems here, and not all of the key counties that you would represent would be those internet-connected systems.

REED: But, effectively, like -- I think what you've said is, that you'd really have to wait for confirmation until the results started coming in on election day, which raises the issue of -- even if you detect it on Election Day, what do we do?

The votes have already been cast. Are you -- is anyone planning on -- what's the -- what reaction we take? How do we notify people? What are -- what steps do they take?

LILES: I'd have to defer to other (OFF-MIKE).

MANFRA: Yes, sir. And I do want to clarify, when we say that that activity would be difficult to detect, it would be -- or difficult to go on undetected, it would -- that we're discussing both at the polling station or the jurisdiction -- that it would be hard for somebody to do that without anybody -- not necessarily that the department would --

would have that immediate insight.
And, to answer your question, yes, that is absolutely something that is a part of our planning and -- and what we would look forward to partnering with the state and local officials on understanding.
REED: So we're, again, about 18 months away from election. We have to be able to develop a -- not technical infrastructure, but an organizational infrastructure that could react, maybe on very short notice, to discovery that actual votes were being tampered. Is that accurate?
MANFRA: Absolutely, sir. It is both technical and organizational.
REED: And do you think there's enough emphasis in terms of the resources and support to do that, the collaboration? I -- you've got 50 states, and among those states, many of the voting jurisdictions are not at the state level -- they're the city and town canvasser. Are we taking it serious enough? I guess that's the issue.
MANFRA: Absolutely, sir. This is one of our highest priorities. And I would also note that we're not just looking ahead to 2018, as election officials remind me, routinely, that elections are conducted on a regular basis. And so -- highest priority, sir. Yes.
REED: Let me ask Mr. Priestap, if I've pronounced it incorrectly., forgive me. But you -- you testified today, and your colleagues, that information was exfiltrated by the Russians. What type of information was taken, and what could it be used for?
PRIESTAP: Yes, sir. I don't want to get into the -- the details of which -- what victim information was taken. Again, we've got a variety of pending investigations.
But it -- it -- again, it could be used for a variety of purposes. Could have been taken to understand what's in those systems. It could have been taken to use to try to target -- learn more about individuals, so that they could be targeted.
It could -- it could have been taken in a way to then publicize, just to send a message, that a foreign adversary has the -- ability to take things and to sow doubt in our voters' minds.
REED: Let me ask you this question, as a judgment. Given the activities that the Russians have deployed, significant resources, constant effort over -- as you -- the intelligence community -- probably a decade, do you think they have a better grasp of the vulnerabilities of the American voting system than you have?
PRIESTAP: I hope not. I think it's a -- I think it's an excellent question and I can -- well, first of all, I hope not and I don't think so, but if they did, I don't think they do anymore.
REED: Thank you very much.
BURR: Thank you, Senator Reed.
Before we move to the second panel, one last question, Mr. Priestap, for you.
Is there any evidence that the attempt to penetrate the DNC was for the purposes of launching this election year intrusion process that they went on? Or was this at the time one of multiple fishing expeditions that existed by Russian actors in the United States?
PRIESTAP: In my opinion, it was one of many efforts. You'd call it a fishing expedition, but to determine again, what's out there, what intelligence can they collect. So they don't go after one place. They go after lots of places and then...
BURR: Tens? Hundreds? Thousands?
PRIESTAP: Hundreds. . At least hundreds.
BURR: OK.
I want to wrap up the first panel with just a slight recap.
I think you have thoroughly covered that there's no question that Russia carried out attacks on state election systems. No vote tallies were affected or affected the outcome of the elections. Russia continues to engage in exploitation of the U.S. elections process and elections are now considered a critical infrastructure, which is extremely important and does bring some interesting potential new guidelines that might apply to other areas of critical infrastructure that we have not thought of because of the autonomy of each individual state and the

control within their state of their election systems.
So I'm sure this will be further discussed as the appropriate committees talk about federal jurisdiction, where that extends to. And clearly, I think it's this committee's responsibility as we wrap up our investigation to hand off to that committee somewhat of a road map from what we've learned or areas that we need to address, and we will work very closely with DHS and with the bureau as we do that.
With that, I will dismiss the first panel and call up the second panel.
END

Subject: Intelligence gathering; Committees; Local elections; State elections; Presidential elections; National security; Democracy; Politics;

Location: Russia United States--US

Company / organization: Name: Federal Bureau of Investigation--FBI; NAICS: 922120;

Publication title: Political Transcript Wire; Lanham

Publication year: 2017

Publication date: Jun 21, 2017

Publisher: CQ Roll Call

Place of publication: Lanham

Country of publication: United States

Publication subject: Political Science

Source type: Wire Feeds

Language of publication: English

Document type: News

ProQuest document ID: 1912737473

Document URL: https://search.proquest.com/docview/1912737473?accountid=14026

Copyright: 2017 Bloomberg Government

Last updated: 2017-06-23

Database: Global Newsstream,ABI/INFORM Trade & Industry

Contact ProQuest
Copyright © 2017 ProQuest LLC. All rights reserved. - Terms and Conditions

Exhibit 32

Report Information from ProQuest

July 12 2017 17:47

18-F-1517//1249

Table of contents

18-F-1517//1244 ProQuest

S INTEL HEARING ON RUSSIAN INTERFERENCE IN 2016 ELECTION, PANEL 2

Publication info: Political Transcript Wire ; Lanham [Lanham]21 June 2017.

ProQuest document link

Links: Check SFX for Availability

Full text: S Intel Hearing on Russian Interference in 2016 Election, Panel 2

JUNE 21, 2017

SPEAKERS: SEN. RICHARD M. BURR, R-N.C. CHAIRMAN SEN. JIM RISCH, R-IDAHO SEN. MARCO RUBIO, R-FLA. SEN. SUSAN COLLINS, R-MAINE SEN. ROY BLUNT, R-MO. SEN. TOM COTTON, R-ARK. SEN. JAMES LANKFORD, R-OKLA. SEN. JOHN CORNYN, R-TEXAS SEN. MARK WARNER, D-VA. VICE CHAIRMAN SEN. RON WYDEN, D-ORE. SEN. MARTIN HEINRICH, D-N.M. SEN. JOE MANCHIN III, D-W.VA. SEN. KAMALA HARRIS, D-CALIF. SEN. DIANNE FEINSTEIN, D-CALIF.

SEN. ANGUS KING, I-MAINE

WITNESSES: CONNIE LAWSON, INDIANA SECRETARY OF STATE, PRESIDENT-ELECT, NATIONAL ASSOCIATION OF SECRETARIES OF STATE

MICHAEL HAAS, MIDWEST REGIONAL REPRESENTATIVE, NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS

J. ALEX HALDERMAN, PROFESSOR OF COMPUTER SCIENCE AND ENGINEERING, UNIVERSITY OF MICHIGAN

STEVE SANDVOSS, EXECUTIVE DIRECTOR, ILLINOIS STATE BOARD OF ELECTIONS

[*] BURR: I now call the second panel to order, and ask those visitors to please take their seats. As we move into our second panel this morning, our hearing is shifting from a federal government focus to a state-level focus. During this second panel, we'll again -- we'll gain insight into the experiences of the states in 2016, as well as hear about efforts to maintain election security moving forward.

For our second panel, I'd like to welcome our witnesses: the Honorable Connie Lawson, president-elect of the National Association of Secretaries of State and the secretary of state of Indiana; Michael Haas, the Midwest regional representative to the National Association of State Election Directors and the administrator of the Wisconsin Election Commission; Steve Sandvoss, executive director of the Illinois State Board of Elections; and Dr. J. Alex Halderman, professor of computer science and engineering, University of Michigan.

Thank you all for being here.

Collectively, you bring a wealth of knowledge and a depth of understanding of our state election systems, potential vulnerabilities of our voting process and procedures and the mitigation measures we need to take at the state level to protect the foundation of American democracy.

In January of this year, then-Secretary of State -- Secretary of Homeland Security Jeh Johnson designated the election infrastructure used in federal elections as a component of U.S. critical infrastructure. DHS stated that the designation of established election infrastructure as a priority within the national infrastructure protection plan.

It enabled the department to prioritize out cybersecurity assistance to state and local election officials for those who requested, it and made it publicly known that the election infrastructure enjoys all the benefits and protections of critical infrastructure that the U.S. government has to offer.

Some of your colleagues objected to this designation, seeing it as federal government interference. Today, I'd like to hear your views on this specifically, but more broadly, how the states and the federal government can best work together. I'm a proud defender of states' rights but this could easily be a moment of divided we fall. We must set aside our suspicions and see this for what it is, an opportunity to unite against a common threat.

18-F-1517//1249

Together, we can bring considerable resources to bear and keep the election system safe. Again, I'd like to thank our witnesses for being here.

And at this time, I'd turn to the vice chairman for any comments he might make.

The vice chairman doesn't have any.

I will assume, Mr. Haas, that by some process, you have been elected to go first? Unless there is an agreement -- which -- where are we going to start?

HAAS: Actually, I think we were going to defer to Secretary Lawson to start, if that's OK with the chair.

BURR: Madam Secretary, you are recognized.

LAWSON: Well, good morning, Chairman Burr and Vice Chairman Warner and distinguished members of the committee. I want to thank you for the chance to appear before you today. It's an honor to represent the nation's secretaries of state, 40 of whom serve as chief state election officials.

I am Connie Lawson, Indiana secretary of state and I'm also president-elect of the bipartisan National Association of Secretaries of State. I'm here to discuss our capacity to secure state and locally run elections from very significant and persistent nation- state cyber threats.

With statewide elections in New Jersey and Virginia this year and many more contests to follow in '18, I want to assure you and all Americans that election officials across the United States are taking cybersecurity very seriously.

First and foremost, this hearing offers a chance to separate facts from fiction regarding the '16 presidential election. As noted many times, we have seen no evidence that vote casting or counting was subject to manipulation in any state or locality, nor do we have any reason to question the results. Just a quick summary of what we know about documented foreign targeting of state and local election systems. In the 2016 election cycle, as confirmed by the Department of Homeland Security, no major cyber security issues were reported on Election Day, November 8.

Last summer, our intelligence agencies found that up to 20 state networks had been probed by entities essentially rattling the door knobs to check for unlocked doors. Foreign-based hackers were able to gain access to voter registration systems in Arizona and Illinois, prompting the FBI to warn state election offices to increase their election security measures for the November election. In more recent days, we've learned from a top-secret NSA report that the identity of a company providing voter registration support services in several states was compromised.

Of course, it's gravely concerning that election officials have only recently learned about the threats outlined in the leaked NSA report, especially given the fact that the formed DHS Secretary Jay Johnson repeatedly told my colleagues and I that no specific or credible threats existed in the fall of '16. It is unclear why our intelligence agencies would withhold timely and specific threat information from election officials.

I have every confidence that other panelists will address voting equipment risk and conceptual attack scenarios for you today. But I want to emphasize some systemic safeguards that we have against cyber attackers.

Our system is complex and decentralized with a great deal of agility and low levels of connectivity. Even within states, much diversity can exist from one locality to the next. This autonomy serves as a check on the capabilities of nefarious actors.

I also want to mention the recent designation of election systems as critical infrastructure. Real issues exist with the designation, including a lack of clear parameters around the order which currently provides DHS and other federal agencies with a large amount of unchecked executive authority over our election's process. At no time between August of '16 and January of '17 did NASS and its members have a thorough discussion with DHS on what the designation means.

Threat sharing had been touted as a key justification for the designation. Yet, nearly six months later, no secretary of State is currently authorized to receive classified threat information from our intelligence agencies. From information gaps to knowledge gaps that aren't being addressed, this process threatens to erode public

confidence in the election process as much as any foreign cyber threat. It's also shredding the rights that states hold to determine their own election procedures subject to the acts of Congress. If the designation ultimately reduces diversity and autonomy in our voting process, the potential for adverse effects from perceived or real cyber effects -- attacks, excuse me -- will likely be much greater and no the other way around. Looking ahead, the National Association -- the NASS Election Security Task Force was created to ensure that state election officials are working together to combat threats and foster effective partnerships with the federal government and other public-private stakeholders. In guarding against cyber threats, the trendline is positive, but more can be done. Most notably, many states and localities are working to replace or upgrade their voting equipment.

If I have one major request for you today, other than rescinding the critical infrastructure designation for elections, it is to help election officials get access to classified information sharing. We need this information to defend state elections from foreign interference and respond to threats.

Thank you. And I look forward to answering your questions.

BURR: Thank you, Secretary Lawson. Who would like to -- Mr. Haas?

HASS: Thank you. Good morning.

Chairman Burr, Vice Chairman Warner and committee members, on behalf of the National Association of State Election Directors, thank you for this opportunity to share what states learned from the 2016 elections and some steps that it will be -- we are taking to further secure our election systems. I serve as Wisconsin's chief election official, and I'm a member of NASS at the executive board.

We do not have a state elected official who oversees elections in Wisconsin. Many of our state election directors across the country are housed in the secretary of state's offices, but some are not.

The 2016 president election reinforced several basic lessons, although sometimes in a new context. For instance, all must understand the importance of constant and effective communication to ensure that all actors have the tools they need. The new twist (ph) in 2016 of course involved communicating about the security of election systems with the Department of Homeland Security as well as the state staff who provide cyber security protection to our voter registration databases.

As we have heard this morning, some states have expressed concerns about the timeliness and the details of communications from Homeland Security regarding potential threats -- security threats to state election systems. The recent reports about attempted attacks on state voter registration systems, which occurred last fall, caught many states by surprise.

We look forward to working with DHS and other federal officials to develop protocols and expectations for communicating similar information going forward. For example, state election officials believe it is important that we be in the loop regarding contacts that DHS has with local election officials regarding security threats such as the spear-fishing attempts that were recently publicized. States should be aware of this information to protect their systems and so that we can provide additional training and guidance to local election officials.

I appreciate the concern that was expressed this morning that this is a two-way street. And we, at the state level, need to also think carefully about how -- how to most effectively communicate with our local election officials if and when there is an incident that we are aware of at the state level. As part of the DHS designation of election systems as critical infrastructure, bodies (ph) such as coordinating counsels can help to facilitate decisions regarding the proper balance between notifying state and local officials, and protecting confidential or sensitive information.

NASED believes that those coordinating bodies should consist of a broad representation of stakeholders. And we have expressed our strong interest to DHS in participating on those bodies. I would also note that the executive board of NASED supports the request of the U.S. Elections Assistance Commission that it serves as the co-sector's specific -- specific agency as the logical federal agency to partner with DHS to provide subject matter expertise and assistance in communicating with local election officials as the EAC has that communication structure already in place.

HASS: The 2016 elections also reinforced the need for constantly enhancing the security of voter registration databases, as we have heard this morning. While hacking into a voter registration system has no effect on tabulating election results, intrusions could result in unauthorized parties gaining access to data, regarding voters, candidates, ballot contests, and polling places.

I would note that while much of that information is public upon request, there may be some confidential data held in those databases, such as the voter's date of birth, the driver's license number, the last four digits of the social security number. Different states have different laws about what pieces of that data is confidential.

The 2016 elections demonstrated that state and local election officials can implement steps to improve the -- the security of voter data, and then (ph) many of these steps are not complicated.

In addition to the cyber hygiene scans and risk assessments, states are implementing greater use of multi-factor authentication, for users of our systems, updating firewalls, the use of white list, to block unauthorized users, and completely blocking access from any foreign IP address.

The final lesson of 2016 I would like to address relates to voting equipment. To be clear, as it has been said many times this morning, there is no evidence that voting machines or election results have been altered in U.S. elections.

I appreciate the committee's emphasis on that. I think that for the public that cannot be states enough, and strongly enough. Still, we as election administrators must exercise vigilance to assure that such theoretical attacks do not become reality, and we must also continue to educate the public about safeguards in the system. Those safeguards include the decentralized structure of elections that we've heard about this morning and the diversity of voting equipment.

Also, in most cases voting equipment is not connected to the Internet, and therefore cannot be attacked through cyber space. Also it is important to keep in mind that 3 out of 4 ballots cast in American elections are on paper ballots. Most ballots cast on touch screen equipment also have a paper trail that voters can immediately verify their votes, and then election officials can use for audits, and recounts.

There are also several redundancies in the testing and certification of voting equipment. It's important to realize that voting equipment is not only used on Election Day. It's functionality is tested several times during the process.

In short, the 2016 election's taught us, that the potential for disrupting election processes in technology, by foreign or domestic actors is a serious and increasing concern. However, we as state election directors, we have had continued cooperation, and more effective communication, along with continued vigilance and innovation, will ensure the integrity of our voting processes and election results.

Again, we look forward to working with our federal partners as we plan for elections going forward. Thank you for the opportunity to share these thoughts and I'd be happy to answer any questions.

BURR: Thank you, Mr. Haas.

Mr. Sandvoss.

SANDVOSS: Good morning. Thank you, Chairman Burr, Vice Chairman Warner, and distinguished members of the committee. As Director of the State Board of Elections, I'd just like to briefly describe what our agency does. We are an independent bipartisan agency created by the 1970 Illinois constitution, charged with general supervision over the election, and registration laws in the state of Illinois.

As all of you seem to be aware, almost a year ago today, on June 23rd, the Illinois State Board of Elections was the victim of a malicious cyber attack of unknown origin, against the Illinois voter registration system database. Because of the initial low volume nature of the attack, the State Board of Election's staff did not become aware of it at first. Almost three weeks later, on July 12th, State Board of Elections IT staff was made aware of performance issues with the IVRS database server. The processor's usage had spiked to 100 percent with no explanation.

Analysis of the server logs revealed that the heavy load was a result of rapidly repeated data base queries on

the application status page of our paperless online voter application website. Additionally, the server log showed the data based queries were malicious in nature. It was a form of cyber attack known as SQL, which is structured query language injection. SQL injections are essentially unauthorized, malicious data base queries entered in to a data field, in a web based application.

We later determined that these SQLs originated from several foreign based IP addresses. SP programmers immediately introduced code changes to eliminate this particular vulnerability in our website. The following day, on July 13th, the SBE IT made the decision to take the website and IVRS database offline to investigate the severity of the attack. SBE staff maintained the ability to log and view all site access attempts.

Malicious traffic from the IP addresses continued, though it was blocked at the firewall level. Firewall monitoring indicated that the attackers were hitting SBE IP addresses five times per second, 24 hours a day. These attacks continued until August 12th, when they abruptly ceased. SV staff began working to determine the extent of the breech, analyzing the integrity of the IVRS database, and introducing security enhancements to the IVRS web servers and database.

A week later, on July 19th, we notified the Illinois general assembly of the security breech, in accordance with the Personal Information Protection Act. In addition, we notified the Attorney General's office. On July 21st, the State Board of Election's IT staff completed security enhancements and began to bring the IVRS system back online. A week after that, on July 28th, both the Illinois registration system, and the paperless online voting application became totally functional once again.

Since the attack occurred, the State Board of Elections has maintained the following ongoing activities the DHS scans the State Board of Election's systems for vulnerabilities, on a weekly basis. The Illinois Department of Innovation and Technology, which is a statewide entity that coordinates the IT systems of many of the Illinois state agencies, continuously monitors activity on the Illinois Century Network, which is the general network that provides firewall protection for the state computer systems.

This Department of Innovation and Technology, also called DOIT, provided cyber security awareness training for all state of Illinois employees, ours included. Now the State Board of Election's IT staff continues to monitor web server, and firewall logs on a daily basis. And in addition a virus protection software is downloaded, also on a daily basis. As a result of informing the Illinois Attorney General's office of the breach, the State Board of Elections was contacted by the Federal Bureau Investigation, and we have fully cooperated with the FBI in their ongoing investigation.

The FBI advised that we work with the Department of Homeland Securities, United States Computer Emergency Readiness team, to ensure that there is no ongoing malicious activity on any of the SBE systems. They also confirmed -- that is, the -- the Department of Homeland Security also confirmed that there's no ongoing malicious activity occurring in SBE computer systems.

To comply with the Personal Information Protection Act, nearly 76,000 registered voters were contacted as potential victims of the data breach. The SBE provided information to these individuals on steps to take if they felt that they were the victims of identity theft.

Additionally, the SBE developed an online tool to inform affected individuals of the specific information that was included in their voter record that may have been compromised.

As far as looking to -- for future concerns, one of the concerns facing our state and many others, we believe, is aging voting equipment. The Help America Vote Act established requirements for voting equipment, while -- but while initial funding was made available to replace the old punch-card equipment, additional funding has not been further appropriated.

If additional funding is not available, we would like to receive authorization to use the states' existing HAVA funds to allow spending on enhanced security across all election-related systems. The IVRS database is a federal mandate through the Help America Vote Act.

Cyber attacks targeting end users are also of particular concern. Security training funded and provided by a

federal entity such as the -- the EAC or DHS would also be beneficial, in our view.
In addition, any guidance or recommendations as to methods for the protection of registration and voting systems from cyber intrusions are always welcome.
Thank you for the time, and I'm happy to answer any questions.
BURR: Thank you, Mr. Sandvoss.
Dr. Halderman?
HALDERMAN: Chairman Burr, Vice Chairman Warner and members of the committee, thank you for inviting me to speak with you today about the security of U.S. elections.
I'm a professor of computer science, and have spent the last 10 years studying the electronic voting systems that our nation relies on. My conclusion from that work is that our highly computerized election infrastructure is vulnerable to sabotage, and even to cyber attacks that could change votes.
These realities risk making our election results more difficult for the American people to trust. I know America's voting machines are vulnerable, because my colleagues and I have hacked them, repeatedly, as part of a decade of research, studying the technology that operates elections and learning how to make it stronger.
We've created attacks that can spread from machine to machine, like a computer virus, and silently change election outcomes. We've studied touchscreen and optical scan systems, and in every single case, we found ways for attackers to sabotage machines and to steal votes. These capabilities are certainly within reach for America's enemies.
As you know, states choose their own voting technology, and while some states are doing well with security, others are alarmingly vulnerable. This puts the entire nation at risk.
In close elections, an attacker can probe the most important swing states or swing counties, find areas with the weakest protection and strike there. In a close election year, changing a few votes in key localities could be enough to tip national results.
The key lesson from 2016 is that these threats are real. We've heard that Russian efforts to target voter registration systems struck 21 states, and we've seen reports detailing efforts to spread an attack from an election technology vendor to local election offices.
Attacking vendors and municipalities could have put Russia in a position to sabotage equipment on Election Day, causing machines or poll books to fail, and causing long lines or disruption. They could have engineered this chaos to have a partisan effect, by striking places that lean heavily towards one candidate.
Some say the fact that voting machines aren't directly connected to the Internet makes them secure, but unfortunately, this is not true. Voting machines are not as distant from the Internet as they may seem.
Before every election, they need to be programmed with races and candidates. That programming is created on a desktop computer, then transferred to voting machines. If Russia infiltrated these election- management computers, it could have spread a vote-stealing attack to vast numbers of machines.
I don't know how far Russia got, or whether they managed to interfere with equipment on Election Day, but there's no doubt that Russia has the technical ability to commit widespread attacks against our voting system, as do other hostile nations. I agree with James Comey when he warned here, two weeks ago, we know they're coming after America, and they'll be back. We must start preparing now.
Fortunately, there's a broad consensus among cybersecurity experts about measures that would make America's election infrastructure much harder to attack. I've co-signed a letter that I ventured into the record from over 100 leading computer scientists, security experts and election officials that recommends three essential steps.
First, we need to upgrade obsolete and vulnerable voting machines, such as paperless touchscreens, and replace them with optical scanners that count paper ballots. This is a technology that 36 states already use. Paper provides a physical record of the vote that simply can't be hacked.
President Trump made this point well on Fox News the morning after -- the morning of the election. He said,

"there's something really nice about the old paper ballot system. You don't worry about hacking."
Second, we need to use the paper to make sure that the computer results are right. This is a common-sense quality control, and it should be routine.
Using what's known as a risk-limiting audit, officials can check a small, random sample of the ballots to quickly and affordably provide high assurance that the election outcome was correct. Only two states, Colorado and New Mexico, currently conduct audits that are robust enough to reliably detect cyber attacks.
Lastly, we need to harden our systems against sabotage and raise the bar for attacks of all sorts by conducting comprehensive threat assessments and applying cybersecurity best practices to the design of voting equipment and the management of elections. These are affordable fixes.
Replacing insecure paperless voting machines nationwide would cost $130 million to $400 million. Running risk-limiting audits nationally for federal elections would cost less than $20 million a year. These amounts are vanishingly small, compared to the national security improvement they buy.
State and local election officials have an extremely difficult job, even without having to worry about cyber attacks by hostile governments. But the federal government can make prudent investments to help them secure elections and uphold voters' confidence. We all want election results that we can trust.
If Congress works closely with the states, we can upgrade our election infrastructure in time for 2018 and 2020. But if we fail to act, I think it's only a matter of time until a major election is disrupted or stolen in a cyber attack.
Thank you for the opportunity to testify today, and for your leadership on this critical matter. I look forward to answering any questions.
BURR: Dr. Halderman, thank you.
The chair would recognize himself for five minutes. Members will be recognized by seniority.
Secretary Lawson, how many states is the secretary of state in charge of the elections process, do you know?
LAWSON: Yes, sir. It's 40. I'm sorry. Yes, sir. It's 40.
BURR: OK. Would you be specific, what do the secretary of states do -- what is it they do not like about elections being designated critical infrastructure?
LAWSON: The most important issue, sir, is that there have been no clear parameters set and even after the three calls that we had with Secretary Jeh Johnson, before the designation was made, we consistently asked for what would be different if the designation was made and how we would communicate. Would it be any different...
(CROSSTALK)
BURR: So nothing has negatively happened except that you don't have the guidance to know what to do?
LAWSON: Nothing has negatively happened to this date, but also, nothing positive has happened.
BURR: Got it. Got it.
Mr. Sandvoss, Illinois is one of the few states that have publicly been identified, I guess that's in part because you took the initiative to do it. You gave a good chronology, 23 June first sign, 12 July state I.T. staff took action, 12 August the attacks stopped.
At what point was the state of Illinois contacted by any federal entity about their system having been attacked or was it the state of Illinois that contacted the federal government?
SANDVOSS: We were contacted by the FBI -- I don't have the exact date but it was after we had referred the matter to the Attorney General's office. My guess would be probably a week after.
BURR: A week after...
(CROSSTALK)
SANDVOSS: After the A.G. was notified by us of this breach.
BURR: And the A.G. was notified approximately when?
SANDVOSS: On July 19th.
BURR: July 19th. OK. At what point did the state of Illinois know that it was the Russians?

SANDVOSS: Actually, to this day, we don't know with certainty that it was the Russians. We've never been told by any official entity. The only one, that we're aware of, that was investigating, was the FBI and they have not told us definitively that it was the Russians. Our I.T. staff was able to identify -- I think it was seven I.P. addresses from a foreign location, I believe it was the Netherlands.

But that doesn't mean that the attack originated in the Netherlands. We have no idea where it originated from.

BURR: Did your I.T. staff have some initial assessments on their own?

SANDVOSS: No, because I think any -- anything of that nature would have been speculative and we didn't want to do that. I think we wanted to leave that to the professional investigators.

BURR: You gave a update on what you're currently doing to enhance the security. DHS weekly security checks. Has the federal -- in your estimation, has the federal government responded appropriately, to date?

SANDVOSS: I believe they have, yes. I've heard nothing from our I.T. division and they'd be the persons that would know. I've heard nothing from them that the DHS's work in that matter has been less than satisfactory.

BURR: Let me ask all of you, except for you, Mr. Sandvoss. Do you believe the extent of cyber threats to election systems should be made public before the next election cycle?

Should we identify those states that were targeted, Mr. Haas?

HAAS: I think as election directors, we're certainly sensitive to the balance that Homeland Security and others need to make. I think so far -- as far as we've gone, we wanted to know, as the victims or potential victims. And then I think as part of the coordinating council and designation of critical infrastructure, there has to be a conversation amongst the election...

(CROSSTALK)

BURR: Is there a right of the public in your state to know?

HAAS: Yes, I believe there is. If there was a hack into our system, I think that our -- we would -- we would certainly want to consult our statutes and so forth, but we would -- we believe in transparency, we would want to let the public know.

BURR: Dr. Halderman?

HALDERMAN: I think the public needs details about these attacks, and about the vulnerabilities of the system, in order to make informed decisions about how we can make the system better and to provide the resources that election officials need. So, yes.

BURR: Secretary Lawson?

LAWSON: I lay awake at night worrying about public confidence in our election systems, and so, I think we need to be very careful and we need to balance the information because the worst thing that we can do is make people think that their vote doesn't count or it could be canceled out.

And so, if telling the public that -- you know, that these attacks are out there and our systems are vulnerable and it doesn't undermine confidence, it makes them know that we are doing everything we possibly can to stop those attacks, I'd be in favor of it.

BURR: I take for granted none of you at the table have evidence that vote tallies were altered in the 2016 election?

HALDERMAN: Correct.

BURR: Dr. Halderman, before I recognize the vice chairman real quickly, when you and your colleagues hacked election systems, did you get caught?

HALDERMAN: We hacked election systems as part of academic research, where we had machines in our facilities...

(CROSSTALK)

BURR: ...I get that. Did you get caught? Did they see your intrusion into their systems?

HALDERMAN: The one instance when I was invited to hack a real voting system, while people were watching, was in Washington D.C. in 2010 and in that instance, it took less than 48 hours for us to change all the votes

and we were not caught.
BURR: Vice chairman?
WARNER: I'd like to thank all the witnesses for their testimony. I find, a little stunning, Mr. Sandvoss, your answer. I don't know -- I think if you saw the preceding panel, you had the DHS and the FBI, unambiguously, say that it was the Russians who hacked into these 21 systems and I find it a little strange that they've not relayed that information to you.
What we discovered in the earlier testimony and that we finally got public disclosure that 21 states were attacked, and under question from -- from Secretary Harris, we found that even though we know those 21 states were attempted to be hacked into, or doors rattled, or whatever analogy you want to use, in many cases, the state election officials, whether the state directors or the secretaries of state, may not even have been notified. I find that stunning. And clearly, lots of local elected officials -- local election officials, where the activities really take place, haven't been notified. So I've got a series of questions and I'd ask for fairly brief responses. Dr. Halderman, can you just again restate, as Senator King mentioned in the earlier testimony, you don't need to disrupt a whole system, you could disrupt a single jurisdiction in a state, and you could, in fact, wipe that ledger clean, you could invalidate potentially not just that local election but then the results at the state -- the congressional level, the states, and ultimately, the nation, is that not correct?
HALDERMAN: Yes, that's correct.
WARNER: So we are not -- while it's important and I believe in our -- the centralized system, we are only as strong as our weakest link. Is that not correct?
HALDERMAN: That's correct.
WARNER: And Mr. Haas, and Secretary Lawson, do you believe that all 21 states that were attacked, that the state election officials are aware?
LAWSON: I can't answer that question, sir. I'm not certain. I will tell you that Indiana has not been notified. I don't know if we're even on the list.
HAAS: I don't know for sure, except that DHS did indicate in a teleconference that all the states that were attacked have been notified.
WARNER: We were told earlier that that's not the case. We were told that they may have been -- the vendors may have been notified. So do you know whether Wisconsin was attacked?
HAAS: We have not been told that -- that we were -- that there was an attack on Wisconsin.
WARNER: Are you comfortable, either one of you, with not having that knowledge?
LAWSON: We are hypersensitive about our security and I would say that when the FBI sent the notice in September, for states to look for certain I.P. addresses to see if their -- their systems had been penetrated, or attempted to be penetrated, we absolutely searched -- in fact, we looked at 15,500,000 log-ins that had happened in our system since the first of January that year.
And so we -- we believe that our system has not been hacked.
HAAS: I would also state that both our office and the chief information officer of the state, and his office, would likely be able to detect that the system was hacked...
(CROSSTALK)
WARNER: Well just, we've got the two leading state election officials not knowing whether their states were one of the 21 that, at least, the Russians probed -- let me finish, please. And you know, I see -- I understand the balance. But the notion that state election officials wouldn't know -- wouldn't know, that local election officials clearly haven't been notified, I appreciate the chairman's offer.
The chairman and I are going to write a letter to all the states. If you view yourself as victims, I think there is a public obligation to disclose. Again, not to re-litigate 2016, but to make sure that we're prepared for 2017, where I have state elections in my state this year, and 2018. And it's -- to do otherwise because there are some -- there are some still in the political process that believe this whole Russian incursion into our elections is a witch

hunt and fake news.
So I could very easily see some local elected officials saying "this is not a problem, this is not a bother. I don't need to tighten up my security procedures at all." And that would do a huge, huge disservice to the very trust, Secretary Lawson, that you say you want to try to present and provide for our voters. So I hope when -- when you receive the letter from our -- and we're going to write this on a confidential basis, but that you would urge your colleagues to come forward, again, not to embarrass any state.
But I find it totally unacceptable, one, that the public doesn't know, that local elected officials -- local election officials don't know that you as two -- as the leaders of the state election officials don't even know whether your states were part of the 21 that has been testified by the DHS that, at least, they were, if not looked at, door jiggled, or actually is the case in Illinois, where actual information from the voter registration efforts were exfiltrated.
So my hope is that you will work with us on a cooperative basis and we want to make sure that the DHS and others are better at sharing at information and you get those classified briefings that you deserve.
BURR: Senator Risch.
RISCH: Thank you very much.
Mr. Sandvoss, I -- July 12th was the date that you first discovered that you had issues. Is that right?
SANDVOSS: Yes, that's correct.
RISCH: And that was a result of a high-volume spike. Is that correct?
SANDVOSS: Yes, that is correct.
RISCH: Then when you looked at it, you found out that the intrusion attempts actually had started June 23rd, is that correct?
SANDVOSS: Yes.
RISCH: So -- and those were low-volume spikes, starting on June 23rd.
SANDVOSS: Yes.
RISCH: All right. So, if they had never cranked up the volume, is it fair to say you would have never discovered it? Or probably wouldn't have discovered it?
SANDVOSS: I would say it would probably not have been discovered -- certainly not right away. And if it was -- the volume was low enough, even an analysis of our server logs might not catch something like that, because it wouldn't stand out.
So I think the answer to your question is yes.
RISCH: Then you said 12 -- or seven days later, the 19th, you notified the attorney general. Is that right?
SANDVOSS: Yes, correct.
RISCH: That was the -- that was the Illinois attorney general, not the U.S. attorney general, is that correct?
SANDVOSS: Yes. State law requires that we notify the attorney general in these instances.
RISCH: So then the next thing that happened is you were contacted by the FBI. Is that correct?
SANDVOSS: Yes.
RISCH: All right. So the question I've got, I'm just -- I'm just trying to get an understanding the facts -- are you assuming that the Illinois A.G. contacted the FBI, or do you know that, or not know that, or (OFF-MIKE).
SANDVOSS: I don't know that for sure, but I -- I would suspect that they probably did, because how else would the FBI know?
RISCH: Right. Well, and that's kind of where I was getting, is that -- that was not the result of some federal analysis -- that there wasn't a federal analysis of this that turned up what had actually happened. Is that -- is that a fair statement?
SANDVOSS: I believe so, yes.
RISCH: You then did some things to try to mitigate what had happened. Had you -- had you shared this with other states, as to what you had done, in order to, I don't know, develop a best practices, if you would?

SANDVOSS: We didn't have any formal notification to all 50 states, no. I think our focus at that time was trying to repair the damage and assess, you know, what needed to be done, especially with respect to the voters who had their, you know, information accessed.

I believe that, once the FBI got -- became aware of this, I know they contacted the different states. I don't believe our attorney general's office did, although I don't know that for certain. But we did not have any formal communication with all 50 states regarding this.

RISCH: And do you believe that you have developed a best- practices action after this attack that you described for us?

SANDVOSS: I believe so, yes.

RISCH: You think it would be appropriate for you to get that out through the secretary of states organization, or other organizations, so that other states could have that.

SANDVOSS: Certainly. Absolutely.

RISCH: OK.

Mr. Halderman, Your hacking that you've described for us -- does -- would your ability -- if you were sitting in Russia right now, wanted to do the same thing that you had done, would that ability be dependent upon the machines, or whatever system is used, being connected to the Internet?

HALDERMAN: That ability would depend on whether pieces of election I.T. equipment -- I.T. offices that are where the election programming is prepared are ever connected to Internet. The machines themselves themselves don't have to be directly connected to the Internet for -- for a remote attacker to target them.

RISCH: So would recommend that -- that the voting system be disconnected from the Internet, that it be a standalone system that can't be accessed from the outside?

HALDERMAN: It's a best practice, certainly, to isolate vote tabulation equipment as much as possible from the Internet, including isolating its -- the systems that are used to program it.

But other peoples of election infrastructure that are critical, such as electronic poll books or online registration systems, do sometimes need to be connected to Internet -- to systems that have Internet access.

RISCH: But that wouldn't necessarily require that it be connected to the Internet for the actual voting process. Is that right?

HALDERMAN: That's right.

RISCH: And then the extrication of that information off of the voting machine -- would that be fair?

HALDERMAN: The -- I think that's fair to say.

RISCH: Thank you.

Mr. Chairman, I think all of this really needs to be drilled down a little bit further, because it seems to me, with this experience, there's probably some really good information where you could put a firewall in place that -- to stop that -- at least minimize it.

Thank you.

BURR: Senator Wyden.

WYDEN: Thank you, Mr. Chairman. And thank -- thank all of you.

I want to start with you, Professor Halderman. What are the dangers of manipulation of voter registration databases, particularly if it isn't apparent until Election Day, when people show up at the polls to vote?

HALDERMAN: I'm concerned that manipulating voter registration databases could be used to try to sabotage the election process on Election Day.

If voters are removed from the registration database, and then they show up on Election Day, that's going to cause -- cause problems. If voters are added to the voter registration database, that could be used to conduct further attacks.

WYDEN: Let me ask, and this can be directed at any of you. I'm trying to get my arms around this role of contractors and subcontractors and vendors who are involved in elections. Any idea, even a ball park number,

of how many of these people there are? Ten, 70, 200?
HALDERMAN: Vendors that host the voter registration system -- I'm sorry, Senator, I don't have a number.
LAWSON: Sir, I don't have an exact number either, but I will -- I will tell you, in Indiana, for an example, we have six different voting system types. Counties make that decision on their own. But they are all certified by our voting system technical oversight program.
WYDEN: That was my main (ph) question.
So somebody is doing certification over these contractors and subcontractors and equipment vendors and the like? Does that include voting machines, by the way? LAWSON: It does. Most states will have a mechanism to certify the voting machines that they're using, the electronic poll books they're using, the tabulation machines that they're using, making sure that they comply with federal and state law, and making sure that they have the audit processes in place.
WYDEN: So you all have a high degree of confidence that these certification processes are not leaving this other world of subcontractors and the like vulnerable?
HALDERMAN: I have several concerns about the certification processes, including that some states do not require certification to federal standards; that the federal standards that we have are unfortunately long overdue for an update and have significant gaps when it comes to security. And that the certification process doesn't necessarily cover all of the actors that are involved in that process, including the day-to-day operations of companies that do pre-election programming.
WYDEN: One last question. We Oregonians and a number of my colleagues are supportive of our efforts to take vote-by-mail national. And we've had it. I was in effect the country's first senator elected by vote-by-mail in 1996. We've got a paper trail. We've got air gap computers. We've got plenty of time to correct voter registration problems if there are any.
Aren't those the key elements of trying to get on top of this? Because it seems to me, particularly the paper trail. If you want to send a message to the people who are putting at risk the integrity of our electoral institutions, having a paper trail is just fundamental to being able to have the backup we need.
I think you're nodding affirmatively, Professor Halderman, so I'm kind of inclined -- or one of you two at the end were nodding affirmatively, and I'll quit while I'm ahead if that was the case -- but would either of you like to take that on?
HALDERMAN: Vote-by-mail has significant cybersecurity benefits. It's very difficult to hack a vote-by-mail system from an office in Moscow. There are -- whether vote-by-mail is appropriate for every state, in every context, is in our system of course a matter for the states, but I think it offers positive security benefits.
WYDEN: All right.
Thank you, Mr. Chairman.
BURR: Senator Blunt?
BLUNT: Dr. Halderman, on that last answer to that last question, how do you count vote-by-mail ballots?
HALDERMAN: Generally, they would be counted using optical scanners.
BLUNT: Exactly. So you count them the same way you count ballots that aren't vote-by-mail in almost every jurisdiction?
HALDERMAN: If the optical scan ballots are subsequently audited, you can get high security from that process, but yes.
BLUNT: Well that's a different -- that's a different question. Your question there is do you prefer paper ballots and an audit trail, and I do too, but let's not assume that the vote-by-mail ballots are counted any differently. They're counted probably at a more central location, but that doesn't mean that all the manipulation you talked about that we need to protect against wouldn't happen in a vote-by- mail election. You've got a way to go back and you've got a paper trail to count.
HALDERMAN: That's correct. There are three things you need: paper, auditing, and otherwise good security

practices.
BLUNT: While I've got you there, on auditing, how would you audit a non-paper system? If it's a touch-screen system, you mentioned Colorado, and New Mexico already did a required sample audit, which I'm certainly not opposed to that if that's what states want to do, or is the best thing to do. How would you do a non-paper audit?
HALDERMAN: Senator, I think it would be difficult or impossible to audit non-paper systems with the technology that we use in the United States, to a high level of assurance.
BLUNT: So even if you -- if you don't have something to audit, it's pretty hard to audit a system that counted -- that didn't leave a trail.
HALDERMAN: It's basically impossible.
BLUNT: So, Mr. Sandvoss, in Illinois, do you certify counting systems?
SANDVOSS: Yes, we do.
BLUNT: And Secretary Lawson, do you certify counting systems?
LAWSON: Yes, sir.
BLUNT: Mr. Haas, in your, your jurisdiction, somebody is certifying those systems that you use?
HAAS: We both rely on the EAC certification and then our commission does a testing protocol and then approves the equipment to be used in the state of Wisconsin.
BLUNT: And back in Illinois, do you then monitor, in any way, that counting system while it's doing the actual counting?
SANDVOSS: No, the actual counting done on Election Day, Election Night, rather, is done locally at the County Clerk's offices or Board of Election Commissioner offices. We certify the voting equipment -- they have to apply for certification and approval, which we conduct a fairly rigorous test of the voting equipment, but then in actual practice, other than -- we do conduct pre-election tests of the voting equipment on a random basis before each election, but there -- it's a limited number of jurisdictions.
BLUNT: And do you do that in a way that allows you, from your central office, to get into the local system? Or do you go to the local jurisdictions or just monitor how they count that -- how they, how they check that counting system?
SANDVOSS: When we do our pre-election tests, we actually visit the jurisdiction.
BLUNT: All right.
Secretary Lawson, similar?
LAWSON: Similar, however, the State does not go into the Counties, but the Counties are required to do a public test, and as I mentioned, it's public. And so they're required to do testing on the machines, the tabulation, there's a bipartisan election board that's there...
(CROSSTALK)
BLUNT: I guess the -- I guess the point I'd want to drive home there is, that not opening that door to the counting system -- if you don't have the door, nobody else can get through that door as well. But there's monitoring, there's local testing, I don't suggest at all that Dr. Halderman's comments aren't important or something we should guard against, it's -- I was an election official for twenty years, including the Chief Election Official for eight of those, and something -- as we were transitioning to these systems -- something I was always concerned about is what could possibly be done that could be done and undetected.
One of the reasons I always liked the audit trail -- that obviously, Dr. Halderman, you do, you do too, is that you do have something to go back -- if you have a reason to go back -- and really determine what happened on Election Day. Let's talk for just a moment about the much more open registration system.
Secretary Lawson, you said you had 15,500 logins. I believe that was -- talk about logging -- what are they logging into, there? The statewide voter registration system that you maintain a copy of?
LAWSON: The 92 County Clerks in Indiana are connected to the statewide voter registration system, and that 15,500,000 logins reflected the work that they did that year.

BLUNT: 15,500,000?
LAWSON: 15,500,000.
BLUNT: So, obviously, that's a system that has lots of people coming in -- in and out of that system all the time. Do local jurisdictions, like if the library does registration, do you have counties where they can also put those registrations directly into the system?
LAWSON: Other than the counties, no sir. But we do have Indianavoters.com, where a voter can go on and register themselves. And it's a record that is compared to the BMV record, and then the counties will find that information in their hopper the next day. And then they will -- or their computer system, and then the next day they will have the ability to determine whether or not the application is correct.
BLUNT: Do all of your jurisdictions, the three jurisdictions here reflected, have some kind of provisional voting, if you get to the voting place on Election Day and your address is wrong, or your name is wrong, or it doesn't occur -- it doesn't appear at all? Do you have a way somebody can cast a ballot before they leave?
LAWSON: Yes, sir.
BLUNT: And in Illinois?
SANDVOSS: Yes, we do.
HAAS: We have provisional ballots, but they are very limited. We are not an NVR -- NVRA state. And we also have Election Day registration, so people can register at the polls.
BLUNT: So, the failure to have your name properly on the -- I understand, Chairman, and I also noticed the time on others. But just -- the registration system is much more open than the tallying system, that doesn't mean the tallying system doesn't need to be further protected. But the registration system, the idea that somebody gets into the registration system -- there are plenty of ways to do that. Unfortunately, we think now other countries and governments may be doing that as well.
BURR: Senator King?
KING: Thank you, Mr. Chairman.
Dr. Halderman, you're pretty good at hacking voting machines, by your testimony. Do you think the Russians are as good as you?
HALDERMAN: The Russians have the resources of a nation-state. I would say their capabilities would significantly exceed mine.
KING: I expected that was going to be your answer, but I wasn't sure whether your modesty would -- but I think that's an important point, because you testified here today that you were able to hack into a voting machine in 48 hours, change the results, and nobody knew you had done it.
And if you could do it, I think the point is, the Russians could do it if they chose. And we've been talking a lot about registrations lists. My understanding is that, quite often, a voter registration list, at some point in the process, is linked up with -- the computer that has the voter registration list, is linked up with configuring the voting machines, and perhaps even tallying votes. Is that true? Can any of you...
(CROSSTALK)
LAWSON: No, sir.
KING: There's -- there's no connection between the registration list and the voting machines?
LAWSON: No.
KING: Illinois? Is that...
(CROSSTALK)
SANDVOSS: Not in Illinois, no.
KING: OK.
HAAS: That's correct. KING: Well, then I was mistaken. Hm?
Yes, Dr. Halderman?
HALDERMAN: I believe that depends on the specific equipment involved. There may be some designs of voting

systems where there -- the sign-in and the vote counting system are linked.
KING: But of course, if, as you testified I think, if the voting registration list is tampered with in some way, on Election Day, it would be chaos. If names disappeared, people arrived at the polls and their names weren't on the list. Isn't that correct, Ms. Lawson?
LAWSON: If a person showed up at the polls to vote and their name wasn't on the list, if they were expecting they would be given a provisional ballot, I think the biggest danger is that the lines at the polls would increase significantly, if there was a large number of folks who had to do that in each precinct.
KING: Right, that was what I was referring to. On August 1st of 2016, press reports have indicated that there was an FBI notification to all of their field offices about the danger of cyber intrusions into voting systems. Supposedly, those were passed on to state election systems. Did you three get something from the FBI around August 1st that gave IP addresses and some warnings about what should be done?
SANDVOSS: Yes, we did receive an FBI flash. It was in August, and you're saying the 1st, I believe that was it.
KING: That was, yeah, I understand that was the date of it.
Ms. Lawson, did you receive that?
LAWSON: Yes, Indiana received a notice from the FBI.
HAAS: We did, as well.
KING: So there is some interconnection. I mean, one of the things that I'm sort of hearing, and I'm frankly appreciative and happy that you all did receive that notice, but there seems to be a lack of information sharing that goes on that we really need to be sure that -- for example, if you learn -- if something happens in Illinois -- some system whereby you can alert your colleagues across the country to look out for this. And if we learn things here in Washington, if the FBI learns things, that they can alert people around the country, because the best time to deal with this is before the election. After the election, or on Election Day, is much more difficult.
Dr. Halderman?
HALDERMAN: Yes, I would support further information sharing.
KING: And then finally, we've talked about what we do about this. Paper trails has come up. Is that the principal defense? Is that -- Dr. Halderman, what if -- I asked the question to the prior panel. What would you tell my elections clerk in Brunswick, Maine, would be the three things most important that they should do, or my secretary of state in Maine, to protect themselves against a threat we know is coming?
HALDERMAN: The most important things are to make sure we have votes recorded on paper, paper ballots, which just cannot be changed in a cyber attack, that we look at enough of that paper in a post- election, risk limiting audit, to know that they haven't -- the electronic records haven't been changed.
And then, to make sure we are generally increasing the level of our cyber security practice. Information sharing is an example of a good and recommended practice, as are firewalling systems and other things that have been suggested.
KING: One final question. Is it possible -- and we -- there are some press reports about this, of a cyber attack on the vendors of these machines, to somehow tamper with the machines before they go out to the states. Is that a risk?
HALDERMAN: I would be concerned about that. And, in fact, the small number of vendors is an example of how our system in practice is not quite as decentralized as it may appear -- that attacks spreading via vendors, or from vendors to their customers, could be a way to reach voting equipment over a very large area.
KING: And there have been press reports that that -- that, in fact, was attempted in 2016.
HALDERMAN: Yes, that's correct.
KING: Thank you, Mr. Chairman. Mr. Chairman, I want to thank you for holding this hearing. This is such important information for the public, and for our democracy. I appreciate your work here.
BURR: Thank you, Senator.
Senator Harris?

HARRIS: Thank you. So there's a saying that I'm sure many of you have heard, which is the -- you know the difference between being hacked and not being hacked, is knowing you've been hacked. And so I appreciate, Dr. Halderman, the recommendations that you and your colleagues have made, because it also seems to cover the various elements of what we need to do to protect ourselves as a country in terms of our elections, which is prevention, and then there's the issue of detection and also resilience.

Once we -- if we discover that we've been manipulated, let's have the ability to stand back up as quickly as possible. So I have a few questions in that regard. First of all, have each of you -- you received the -- for the states -- received a notification from the FBI? Is that correct?

LAWSON: Yes, ma'am. HAAS: Yes, yes.

SANDVOSS: Yes.

HARRIS: And were any of you also notified by DHS?

Mr. Sandvoss?

SANDVOSS: We had communications with DHS, I don't recall how they were initiated. But I do know that there have been some -- the conference calls with them, and it may have been through the FBI that that occurred.

HARRIS: And I'm speaking of before the 2016 election.

SANDVOSS: Yes.

HARRIS: Yeah.

SANDVOSS: Yes.

HARRIS: Secretary Lawson?

LAWSON: Yes, we had -- we did have conversations with Department of Homeland Security. However, it was through our national association, it was not a direct contact with the state.

HARRIS: Thank you.

HAAS: We were one of the states that took up DHS on their offers to do the cyber hijinks scan. We did have a number of communications with, I believe, a point person in their Chicago office. The FBI alert I think was about a specific incident, but our communications with DHS were more about general steps that could be taken to protect our systems.

HARRIS: So, as a follow-up to this hearing, if each of you -- to the extent that you can recall the nature of those conversations with DHS before the election, if you could share that with the committee, that would be helpful, so we can figure out how notifications might be more helpful to you in the future. If -- hopefully they're not necessary, but if necessary.

Can you, Ms. Lawson, tell me -- Secretary Lawson -- what, in your opinion, are the pros and cons of requiring states to report to the federal government if there's been a breach or a hack? What can you imagine would be the pros and cons of a policy that would require that?

LAWSON: Well, the pro would be that if there -- if, for an example, the FBI or the Department of Homeland Security has better ways to counter those attacks, or to make sure that the reconnaissance is done after such an attack is more sophisticated than the states, then obviously, that would be a pro. Indiana did not take the opportunity to have DHS do our cyber cleaning because we felt that we were in better shape than what they could provide for us, so that would be the con.

HARRIS: OK. And can you, Professor Halderman, tell me -- you know we -- before this last election cycle, there had been a lot of talk through the years, in various states -- Senator Blunt, I'm sure you were part of those discussions about the efficacy of online voting, because it would bring convenience, speed, efficiency, accuracy -- and now we can see that there will be great, potentially, vulnerabilities by doing that. So can you talk with me a little about -- just in terms of policy -- is the day of discussing the need for online voting, has that day passed because of the vulnerabilities that are associated with that?

HALDERMAN: I think that online voting, unfortunately, would be painting a bullseye on our election system. Today's technology just does not provide the level of security assurance for an online election that you would

need in order for voters to have high confidence.
And I say that, having myself done -- hacked an online voting system that was about to be used in real elections, having found vulnerabilities in online voting systems that are used in other countries. The technology just isn't ready for use.
HARRIS: And isn't that the irony, that the professor of computer engineering -- and I would -- always believed that we need to do more to adopt technology, that government needs to adopt technology -- I think we're advocating good old days of paper voting are the way to go, or at least an emphasis on that, instead of using technology to vote.
Can you tell me also -- any of you, if you know -- it's my understanding that some of the election system vendors have required states to sign agreements that prevent or inhibit independent security testing. Are you familiar with that?
HALDERMAN: That certainly had been something that inhibited attempts by researchers like me to study election systems in the past.
HARRIS: And do you believe that that's a practice that is continuing?
HALDERMAN: I do not -- I don't know the answer to that question.
HARRIS: Have any of you had that experience with any of your vendors?
SANDVOSS: In Illinois, no, we have not. And I don't think Illinois law would allow such an agreement.
LAWSON: I don't believe that would happen in Indiana either, Senator, because in order to sell voting equipment in the state of Indiana, it has to be certified.
HARRIS: Right, which would require testing.
LAWSON: Yes, which requires testing. HARRIS: Thank you, thank you, Mr. Chairman. Thank you.
BURR: Thank you, Senator Harris.
Any Senators seek additional questions or time? Seeing none, let me wrap up. I want to thank all of you for your testimony today.
Secretary Lawson, to you. I really encourage you, as the next representative of secretaries of states, to remain engaged with the federal government, specifically the Department of Homeland Security. And I think with any transition of an administration, there is a handoff and a ramp-up. And I've been extremely impressed with our witness from DHS, who not only was here today, but she has taken the bull by the horns on this issue, and I think you'll see those guidelines very quickly, and I hope that there will be some interaction between secretary of states, since in 40 states you control the voting process.
And you can find the system of federal guidance and collaboration that works comfortably with every secretary of state in your organization. I think it is absolutely critical that we have not only a collaboration, but a communication between the federal government and the states as it relates to our voting systems. If not, I fear that there would be an attempt to, in some way, shape or form, nationalize that.
That is not the answer, and I'll continue to point, Mr. Sandvoss, to Illinois. It is a great example of a state that apparently focused on the IT infrastructure, in staff, and didn't wait for the federal government to knock on the door and say, hey, you got a problem. You identified your problem, you began to remediate it. At some point, the federal government came in as a partner, and I think where we see our greatest strength is to work with states and to chase people like you, Dr. Halderman, who like to break into -- no, I'm just kidding with you. Listen, I think what you did is important.
And I think the questions that you raised about the fact that you really can target to make the impact of what you're trying to do very, very effective. And that's clearly what campaigns do every day. So we shouldn't be surprised if the Russians actually looked at that, or anybody else who wants to intrude into our voting system and our democracy in this country. The -- I've got to admit that the variation of voting methods, six in Indiana, where I don't know how many counties you've got -- I've got 100 counties in North Carolina -- it may be that I find out that every county in North Carolina has the power to determine what voting machines, what voting

software they have.

This can get extremely complicated. Short of trying to standardize everything, which I don't think is the answer, is, how do we create the mechanism for the federal government to collaborate directly with those heads of election systems in the states, and understand up front what we bring to the table, and how we bring it so that we're all looking at the same thing -- the integrity of every vote going to exactly who it was intended to do. So we're going to have debates on paper or electronic, we're going to have debates on what should the federal role be -- at the end of the day, if we haven't got cooperation, and collaboration and communication, I will assure you we will be here with another Congress, with another makeup of the committee, asking the same questions, because we won't have fixed it.

But I think that what Dr. Halderman has said to us is, there are some ways that we can collectively approach this, to where our certainty of intrusions in the future can go down. And the accuracy of the vote totals can be certified. So I thank all the four of you for being here today in our second panel. This hearing is now adjourned.

END

Subject: State elections; Voting machines; Collaboration; National security;

Location: United States--US

Company / organization: Name: National Association of Secretaries of State; NAICS: 813910;

Publication title: Political Transcript Wire; Lanham

Publication year: 2017

Publication date: Jun 21, 2017

Publisher: CQ Roll Call

Place of publication: Lanham

Country of publication: United States

Publication subject: Political Science

Source type: Wire Feeds

Language of publication: English

Document type: News

ProQuest document ID: 1912764930

Document URL: https://search.proquest.com/docview/1912764930?accountid=14026

Copyright: 2017 Bloomberg Government

Last updated: 2017-06-23

Database: Global Newsstream,ABI/INFORM Trade & Industry

Contact ProQuest

Copyright © 2017 ProQuest LLC. All rights reserved. - Terms and Conditions

18-F-1517//1262

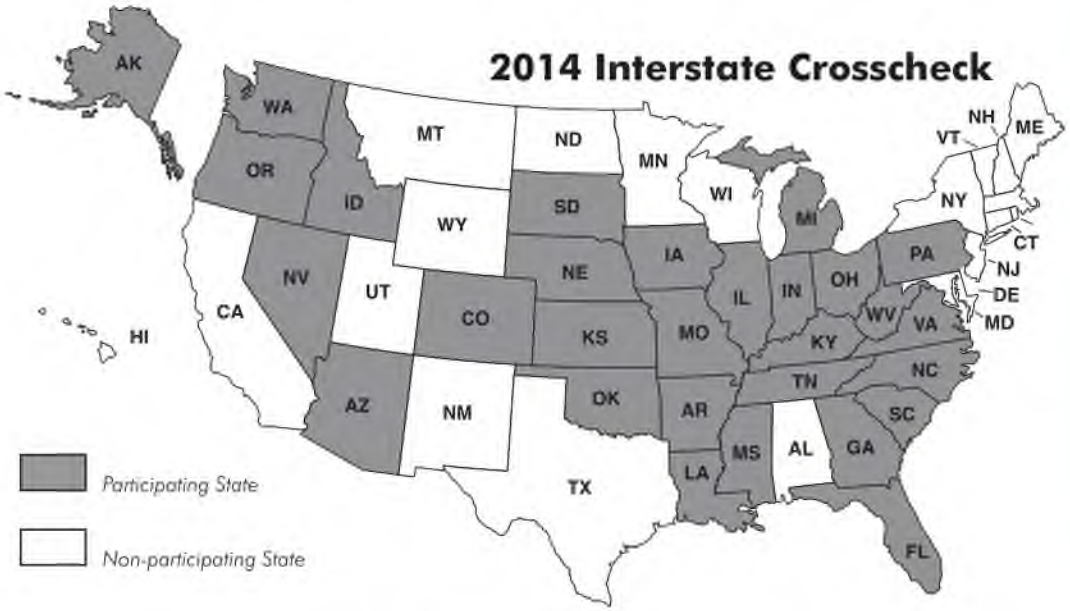
Exhibit 33

canvassing kansas
AN UPDATE ON ELECTION NEWS FROM THE KANSAS SECRETARY OF STATE'S OFFICE

DECEMBER
2013

Interstate Crosscheck Program Grows

The ninth annual data comparison for the interstate voter registration crosscheck program will be run in January 2014. The program has grown from its original four midwest states (Iowa, Kansas, Missouri and Nebraska) to 29 states in 2014. In 2012 there were 15 participating states and in 2013 there were 22.



The interstate crosscheck program, administered by the Kansas Secretary of State's office, began in December 2005 when the secretaries representing the four original states signed a Memorandum of Understanding to coordinate their offices' efforts in several areas of election administration. Crosschecking voter registration data was one of the areas cited. The first crosscheck was conducted the next year, in 2006.

The program serves two purposes: (1) it identifies possible duplicate registrations among states, and (2) it provides evidence of possible double votes. Most states, including Kansas, process the duplicate registrations by mailing the individuals confirmation notices (as provided in the National Voter Registration Act of 1993) and placing the individuals' names in inactive status. Inactive voters are those for whom election officers have received evidence that they have moved out of the county or state. Once they are given inactive status, their registrations may be canceled if they fail to vote or otherwise contact the election office from the date of the confirmation notice through the second succeeding federal general (November) election.

Cont'd on pg. 6

IN THIS ISSUE

18-F-1517//1264

canvassing kansas

Published by the Office of the Secretary of State

EDITORS
Brad Bryant
Kay Curtis

LAYOUT AND DESIGN
Todd Caywood

CONTRIBUTORS
Brad Bryant
Kay Curtis

Suggestions or comments? Please call (785) 368-8095.

This publication may be duplicated for informational purposes only. No written permission is required with the exception of articles or information attributed to a source other than the Kansas Secretary of State.

© 2013

Kansas Secretary of State
Memorial Hall
120 SW 10th Ave.
Topeka, KS 66612-1594
(785) 296-4564

From the desk of the Secretary

"Lead, follow, or get out of the way."
Thomas Paine, 1737 - 1809. Kansas has consistently chosen the former when it comes to elections.

In 2005 Kansas took the lead when four states agreed to compare voter registration records with each other annually in order to identify duplicate voter registrations and double votes. Our IT department pulls data from a secure FTP site, runs comparisons and uploads the results to the FTP site on January 15 each year. Then each participating state can download its results and process them according to their own laws and regulations. The Interstate Voter Registration Crosscheck Program had increased to 14 participating states when I took office in 2011.

Convinced of the value of the program, I decided that I would make it one of my highest priorities to increase the number of participating states, hopefully doubling its size. The more states that participate, the more duplicate records each participating state can find. I contacted chief election officers in other states to explain how Crosscheck works and the value of this tool to maintain clean, current, and accurate voter lists to fight voter fraud. As a result, the number of states participating has more than doubled to 29 states that will share voter registration data in January 2014. While I am very pleased that over half of the 50 states are currently on board, I will continue to promote Crosscheck as an effective means of list maintenance.

In 2008 Kansas took the lead in helping voters to find election information when they need it by using internet search engines. As part of the Voting Information Project (VIP), Kansas contracted with ES&S to make programming changes to our ELVIS database so that all states with ES&S can provide a data feed to the VIP program which hosts the data. Google acknowledged our contribution by presenting a Kansas-shaped VIP award to the State of Kansas at the summer NASS conference.

Finally, in 2011 Kansas took the lead as the first state to combine three election-security policies: (1) requiring a government-issued photo ID for voting in person, (2) requiring either a Kansas driver's license number or photocopy of a current photo ID for applying for a mail-in ballot, and (3) requiring a document proving U.S. citizenship when a person registers to vote for the first time. Consequently, Kansas elections are the most secure in the nation against fraud.

Thank you for all you have done to help implement these reforms. Together we have made Kansas the nation's leader.

Kris W. Kobach

18-F-1517//1265

Voting Information Project Award Received at NASS

On July 19th, 2013, Google presented an award to recognize Kansas' efforts to improve the efficiency and effectiveness of elections through open data. Eight other states also received the award at the National Association of Secretaries of State 2013 Summer Conference in Anchorage, Alaska. Each of the nine states had participated in the Voting Information Project (VIP) by publishing polling places and other election data as part of the open data effort. Secretary of State Kris Kobach was present to accept the award for his office.

By joining the project on the ground floor, Kansas was among the first states to help registered voters to more readily find election information when they need it and where they are most likely to look for it. Government websites often are not the first place voters look. VIP is similar to the online VoterView feature of the Kansas voter registration system, and voters who perform Google searches for voter registration information will end up at the VoterView website as a result of the VIP.

In the run up to the 2012 general election, 22 million times users queried the Google Civic Information API. According to the VIP program, "When the project started in 2008, nobody involved knew whether the open data effort would have any impact at all. Early adopters took a risk on something new by agreeing to participate and the payoff was immense."

Google award presented to the state of Kansas for its contribution to the Voting Information Project.
Photo by Todd Caywood

The VIP program was initiated as a cooperative effort between the Pew Foundation and Google. As a private charitable organization, Pew's rules do not allow them to pay money to a private for-profit corporation, so Pew asked the Kansas SOS office to serve as a go-between. The SOS office wrote specifications and requested Election Systems & Software to make the required programming changes in the voter registration database. The cost of the programming was paid by Pew to the SOS office and passed on to ES&S. As a result, all states with ES&S databases benefit from the new functionality.

For more information about Kansas participation in the VIP project since 2008, see Canvassing Kansas, September 2010, page 6. ■

Clemens Receives CERA Certification

Crystal Clemens, Seward County Deputy Clerk/Election Officer, completed the Election Center's CERA program this year. Certificates were presented at the Election Center's annual national conference in Savannah, GA, held August 13-17, 2013. Crystal was one of fifty eight election officials to receive the award this year.

CERA (Certified Elections/Registration Administrator) is one of very few nationally recognized programs providing professional training for election administrators. The Election Center itself is a nationwide professional association of local, county and state voter registrars and election administrators that promotes training and best practices, monitors and lobbies on federal legislation, and provides a forum for the exchange of ideas.

Completion of the CERA program requires travel and attendance at a number of training sessions across the country over a period of years. Crystal is one of a small handful of Kansas election officials who have completed it.

Crystal's supervisor, Seward County Clerk Stacia Long, had this to say: "Crystal has always shown great passion for the entire election process. I am very proud of her designation as a CERA. She truly is a great asset to the Election Office and Seward County." ■

Attorney General Issues Opinion on Concealed Carry

The office of Attorney General Derek Schmidt issued a formal opinion on November 27, 2013 in response to questions posed by Secretary of State Kris Kobach. Kobach requested the opinion in a letter dated September 30, 2013, as chief state election officer and on behalf of county election officers across the state.

The issue at the heart of the request was how polling places would be affected by passage of the Personal and Family Protection Act of 2013. The Act, passed as Senate Substitute for House Bill 2052 (2013 Kansas Session Laws, Chapter 105), authorizes persons who possess concealed carry permits to carry weapons into municipal buildings except under specific circumstances. "Municipal building" includes any facility owned or leased by a municipality, which could include facilities used as polling places during advance voting or on election day.

In his letter, Secretary Kobach asked the following questions:

1. ***Does the Act apply to privately-owned facilities used as polling places by verbal agreement?***

2. ***Does the Act apply to privately-owned facilities used as polling places by written agreement when no rent money is paid to the owner or manager of the site?***

3. ***Does the Act apply to privately-owned facilities used as polling places by written agreement when rent money is paid to the owner or manager of the site?***

4. ***If only one room or one portion of a building otherwise not subject to the Act is used as a polling place, does the Act apply to the entire building or only to the area used as a polling place?***

5. ***If an area in a nursing home, assisted living center or long term care facility is used for mobile advance voting pursuant to K.S.A. 25-2812, does the Act apply to the voting area?***

6. ***Do the provisions of the Act applicable to schools still apply to school facilities used as polling places?***

7. ***Is a county government liable for claims of denial of equal protection if various polling places have different levels of security as a result of implementation of the Act?***

At the time of this writing, the secretary of state had just begun to analyze the opinion. The SOS office will communicate further information to CEOs when the analysis is complete. In the meantime, CEOs are encouraged to discuss the opinion with their county attorneys and counselors. The full opinion may be found online: ***http://ksag.washburnlaw.edu/opinions/2013/2013-020.pdf***.

The synopsis from Attorney General Opinion 2013-20 is reproduced here:

Except as described herein, the use of real property as a polling place does not transform the nature of that property for the purposes of the PFPA. Any concealed carry requirements that applied to that property immediately before its temporary use as a polling place continue to apply during its use as a polling place and thereafter.

The Personal and Family Protection Act (PFPA) authorizes concealed carry licensees to carry a concealed handgun into a polling place to the extent that concealed handguns are permitted to be carried into the building in which the polling place is located.

The provisions of K.S.A. 2013 Supp. 75-7c20 apply only to buildings that are owned or leased in their entirety by the state or a municipality. If the PFPA requires concealed carry to be permitted in a state or municipal building, then concealed carry licensees must be permitted to carry a concealed handgun in all parts of the building, including areas used as polling places, with the exception of courtrooms, ancillary courtrooms, and secure areas of correctional facilities, jails and law enforcement agencies.

The governing body or chief administrative officer, if no governing body exists, of a state or municipal building may exempt the building from the provisions of K.S.A. 2013 Supp. 75-7c20 for a set period of time. If a state or municipal building is so exempted, concealed carry may be prohibited by posting the building in accordance with K.S.A. 2013 Supp. 75-7c10.

Cont'd on pg. 6

18-F-1517//1267

SOS Office Involved in Litigation

The office of the Kansas Secretary of State finds itself involved in three lawsuits that could affect the voter registration process and the 2014 elections. All are related to the 2011 Kansas SAFE Act. One case deals with the photo ID requirement and the other two deal with the requirement that new voters prove their U.S. citizenship the first time they register to vote.

1. Arthur Sprye and Charles Hamner v. Kris W. Kobach
In a suit filed November 1, 2013, two Osage County voters challenged the constitutionality of the photo ID requirement.

2. Kris W. Kobach, Kansas Secretary of State; and Ken Bennett, Arizona Secretary of State; v. United States Election Assistance Commission
In a suit filed in U.S. District Court in Kansas on August 21, 2013, the Kansas and Arizona Secretaries of State asked for a ruling to require the Election Assistance Commission to include the citizenship requirement in the voter instructions accompanying the universal federal voter registration application form, which is prescribed by the EAC. This lawsuit is in response to the June 17, 2013 ruling by the U.S. Supreme Court in Arizona v. Inter Tribal Council of Arizona regarding the constitutionality of states' requirements that voters provide proof of citizenship. The Court's ruling indicated that states might file suit if the EAC declined to make the necessary changes to the voter registration form administratively.

3. Aaron Belenky, Scott Jones, and Equality Kansas v. Kris Kobach, Kansas Secretary of State, and Brad Bryant, Kansas Elections Director
In a suit filed November 21, 2013, the plaintiffs seek declaratory and injunctive relief to keep the secretary of state's office from implementing a dual voter registration system. The SOS office had developed contingency plans to administer voter registration and ballots to individuals who attempted to register using the universal federal form but who had not provided proof of U.S. citizenship in compliance with Kansas law. No actions have been taken to implement the plan, and no federal elections have occurred in which federal-only ballots were administered to these voters. (See also Canvassing Kansas, September 2013, page 1.)

The goal of the secretary of state's office is to have the cases decided as soon as possible so CEOs and poll workers will know the rules before preparations begin for the 2014 election season. ■

Kobach Reappoints Lehman

Secretary of State Kris Kobach reappointed Tabitha Lehman as Sedgwick County Election Commissioner in September 2013. Her regular term expires on July 19, 2017. This will be Lehman's first full term as election commissioner, having been appointed to fill an unexpired term in 2011.

Lehman was appointed in November 2011 to succeed Bill Gale who resigned his position to pursue other employment. Gale had been appointed in November 2003 to succeed Marilyn Chapman, and he was reappointed in July 2009.

Speaking of her reappointment, Lehman said:
"I appreciate the opportunity to continue serving the voters of Sedgwick County and look forward to providing them with safe and efficient elections in the coming four years." ■

Sedgwick County Election Commissioner Tabitha Lehman
Photo courtesy of Tabitha Lehman

Crosscheck
Cont'd

Evidence of double votes is presented to law enforcement officers for investigation and possible prosecution. The referral is usually made to county law enforcement officers, but state or federal officials may be involved in some cases.

States join the crosscheck by signing a Memorandum of Understanding. The chief state election officer (usually the secretary of state) or a designee may sign the MOU for a given state.

Participating states pull their entire voter registration databases and upload them to a secure FTP site on January 15 each year. The Kansas SOS office IT staff pull the states' data from the FTP site, run the comparison, and upload each state's results to the FTP site. Each state then pulls its results from the FTP site and processes them according to its individual laws, regulations and procedures. In Kansas, results are provided to CEOs with instructions for analyzing them and mailing confirmation notices.

The crosscheck program is one of several list maintenance programs used to keep registration records up to date. (See also Canvassing Kansas, March 2010, page 9.) ■

Attorney General
Cont'd

If the governing body or chief administrative officer of a state or municipal building does not exempt a building from the provisions of K.S.A. 2013 Supp. 75-7c20, then concealed carry licensees must be permitted to carry a concealed handgun inside the building unless adequate security measures are provided and the building is posted as prohibiting concealed carry.

Concealed carry is not required to be permitted in a polling place located inside a privately-owned building unless the county has leased the entire privately-owned building.

Concealed carry is not required to be permitted in polling places located inside public school district buildings because a public school district is not a municipality for the purposes of the PFPA.

An equal protection claim against a county based upon the varying ability of concealed carry licensees to carry a concealed handgun into a polling place would be subject to the rational basis test. ■

Jury List Program Initiated

A 2013 law which went into effect July 1, 2013, requires district courts in Kansas to provide to the secretary of state the names of prospective jurors who indicate on their jury questionnaires that they are not United States citizens. Noncitizens are exempt from jury duty. The secretary of state passes the names on to CEOs for review. If they are found to be registered voters, their registrations are canceled. (See 2013 House Bill 2164; 2013 Kansas Session Laws Chapter 85.)

The relevant section of the law is New Section 1, reproduced below. Most of the bill deals with grand juries.

New Section 1. (a) On and after July 1, 2013, any jury commissioner that receives information regarding citizenship from a prospective juror or court of this state that disqualifies or potentially disqualifies such prospective juror from jury service pursuant to K.S.A. 43-156, and amendments thereto, shall submit such information to the secretary of state in a form and manner approved by the secretary of state. Any such information provided by a jury commissioner to the secretary of state shall be limited to the information regarding citizenship and the full name, current and prior addresses, age and telephone number of the prospective juror, and, if available, the date of birth of the prospective juror. Any such information provided by a jury commissioner to the secretary of state shall be used for the purpose of maintaining voter registrations as required by law.

The secretary of state's office worked with the Office of Judicial Administration (OJA) to design the following procedure to comply with the law:

- The clerk in each of Kansas' 31 judicial districts will submit a monthly report directly to the SOS office containing names of persons who were exempted from jury duty on the basis of their claims to be non-U.S. citizens.
- Reports will be submitted via email on or after the 15th of each month beginning in December 2013.
- The SOS will notify OJA of missing reports. OJA will contact any such district court clerks to remind them to submit their reports.
- If any of the persons listed in the reports are found to be registered voters and their citizenship status is not in doubt, their names will be sent by the SOS office to the appropriate county election officers with instructions regarding the possible cancellation of the persons' voter registration records. ■

18-F-1517//1269

State Fair Opinion Poll Results

The Office of the Secretary of State has operated a booth in the Meadowlark Building at the Kansas State Fair in Hutchinson for more than 25 years. The dates of the fair this year were September 6-15. This was the 100th anniversary of the fair, and the theme was "Never Gets Old."

At the booth, the SOS office provides information about agency activities, registers voters, and conducts an opinion poll on current issues. Don Merriman, Saline County Clerk, has assisted the SOS office for many years by lending ES&S iVotronic voting machines to help the fair visitors familiarize themselves with electronic voting technology. We want to recognize and thank Don for his assistance and the Lockwood Company for its donation of ballot programming services.

The SOS booth is mostly staffed by agency employees, but sometimes county election office personnel help out by volunteering to work in the booth. This year's county volunteers were: Sharon Seibel, Ford County Clerk; Debbie Cox, Ford County Deputy Clerk; Donna Maskus, Ellis County Clerk; Don Merriman, Saline County Clerk; Crysta Torson, Lane County Clerk; and Karen Duncan, Lane County Deputy Clerk. Thanks to the volunteers for helping out!

Following are the results of the opinion poll:

Question #1: New Kansas voters must provide proof of citizenship when registering to vote.

709 *I approve of this requirement.*
96 *I do not approve of this requirement.*
27 *I have no opinion about this requirement.*

Question #2: Which university will advance the furthest in the 2014 NCAA Men's Basketball Tournament?

397 *University of Kansas*
196 *Kansas State University*
179 *Wichita State University*
48 *None will make the tournament*

Question #3: Which of these alleged abuses of power by the federal government is the most concerning to you?

342 *NSA secretly collecting phone records of millions of U.S. citizens.*
332 *IRS intentionally discriminating against conservative organizations.*
153 *Presidential political appointees using secret email accounts to conduct official government business.*
132 *White House's sweeping seizure of Associated Press records and cable television documents.*

Question #4: Should the Internal Revenue Service be abolished?

526 *Yes. A flat or fair tax is simpler, cheaper and easier to manage.*
86 *Yes. We shouldn't have to pay income tax anyway.*
125 *No. Better training and oversight will fix most problems.*
2 *No. There is nothing wrong with the IRS.*

Question #5: Who is your favorite super hero?

90 *Xena: Warrior Princess*
379 *Superman*
94 *Wonder Woman*
195 *Batman* ■

Former Longtime Neosho County Clerk Dies

Wayne B. Gibson, Jr., a well known longtime county clerk from Neosho County, died on September 18, 2013, at a hospital in Labette County. Wayne served many years in the Neosho County Clerk's office and was known to Kansas election officials as a hardworking, conscientious public servant.

Gibson started working in the county clerk's office on January 16, 1961 and became Deputy Clerk about a month later. He then became Clerk on July 14, 1971, following the death of his predecessor, Virgil Lowe. Gibson served continuously until his retirement on April 20, 2007. During that time he was elected ten times - in 1972, 1974, 1976, 1980, 1984, 1988, 1992, 1996, 2000 and 2004.

The vacancy created by Gibson's resignation was filled by Randal Neely, who took office on August 1, 2007, and continues in office today. ■

Dominion Seeks Voting System Certification

Dominion Voting Systems, Inc., submitted a letter dated October 4, 2013 requesting certification of its Democracy Suite Version 4.14 voting system. According to Kansas law, a manufacturer seeking certification of its voting system must submit a formal letter, pay a $500 fee, and demonstrate the system at a certification hearing held in Topeka.

A hearing was held at the secretary of state's office on November 21, 2013, attended by Secretary of State Kris Kobach and members of his staff. The Democracy Suite system was demonstrated and explained by Norma Townsend, Don Vopalensky, Jeff Hintz and Michael Kelava. Dominion is represented in Kansas by its subcontractor, Election Source. Dominion also markets and services Premier (formerly Diebold) voting equipment, having purchased Premier from Election Systems and Software several years ago. ES&S still sells and services Premier equipment along with its own system, but Dominion owns the intellectual property rights of Premier equipment as a result of its purchase of the company.

As of this writing, Secretary Kobach has not certified the Dominion Democracy Suite. CEOs will be notified if and when certification is granted.

The Democracy Suite is a paper optical scan-based system which includes precinct ballot scanners and central scanners. The accessible ADA- and HAVA-compliant device allows a voter with a visual impairment to record his/her choices using an audio ballot and keypad. The system prints an optical scan ballot that is scanned along with other ballots. ■

Sedgwick County Sued Over Ballot Records

Sedgwick County Election Commissioner Tabitha Lehman was sued by a person seeking public access to Real Time Audit Logs (RTALs) on electronic voting machines. RTAL is ES&S's trade name for a voter verifiable paper audit trail (VVPAT), which is a printable electronic record of each voter's actions on the voting machine. RTAL documents are viewable by the voter before the electronic ballot is cast. Once the voter has cast the ballot the documents are randomly stored in the system's memory.

Elizabeth Clarkson v. Sedgwick County Elections Commissioner Tabitha Lehman was filed in state district court in Sedgwick County on June 18, 2013. The plaintiff sought access to RTAL records pursuant to the Kansas Open Records Act in order to conduct a post-election audit of the results of the November 2010 election.

In response to the plaintiff's original request for records, the election office provided precinct-based results tapes but denied the request for individual ballot logs, citing K.S.A. 25-2422 and the unnecessary burden and expense required to produce the records. State law does provide limited access to election records in a recount, but the law does not have specific provisions related to VVPATs or RTALs. These arguments were detailed in a response filed in court in July.

The court ruled in favor of the election commissioner's office. ■

SOS Holiday Hours

In observance of the regular calendar of state holidays, the secretary of state's office will be closed on the following dates:

December 25, 2013, for Christmas Day, and **January 1, 2014,** for New Year's Day.

In addition, the office will be closed Monday, **January 20, 2014** in observance of Martin Luther King, Jr. Day.

Happy Holidays from the SOS office!

18-F-1517//1271

Exhibit 34

Interstate Voter Registration Crosscheck Program

National Association of State Election Directors

January 26, 2013

Kris W. Kobach

18-F-1517//1273

National Voter Registration Act of 1993

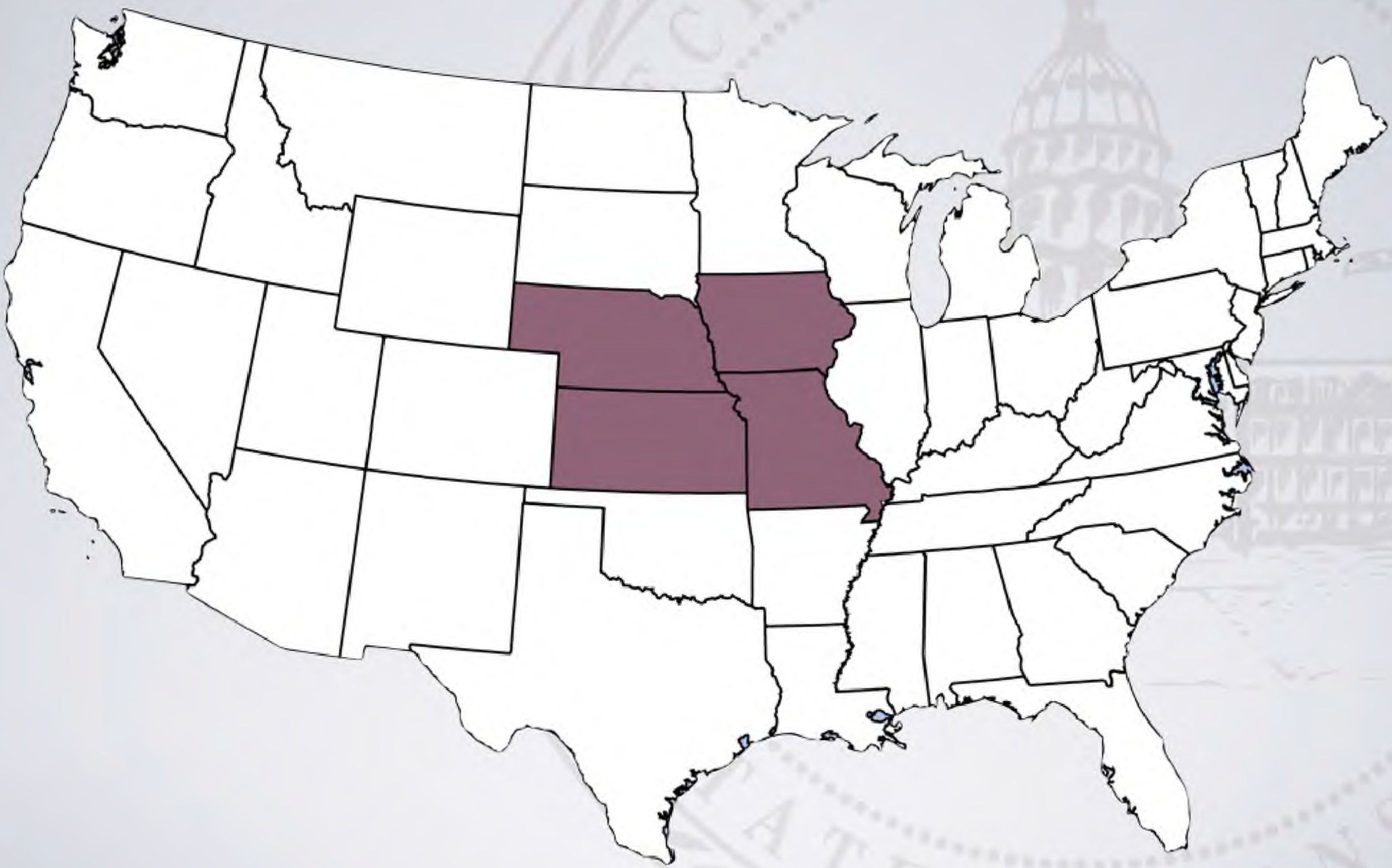
- **Section 2 Findings and Purposes**
- (b) Purposes
- (1) to establish procedures that will increase the number of eligible citizens who register to vote in elections for Federal office;
- (2) to make it possible for Federal, State, and local governments to implement this subchapter in a manner that enhances the participation of eligible citizens as voters in elections for Federal office;
- (3) to protect the integrity of the electoral process; and
- **(4) to ensure that accurate and current voter registration rolls are maintained.**

From the Federal Election Commission's guide: Implementing the National Voter Registration Act of 1993:

The features (of the National Voter Registration Act) include a requirement that states "conduct a general program" the purpose of which is "to protect the integrity of the electoral process by ensuring the maintenance of an accurate and current voter registration roll for elections for Federal office"

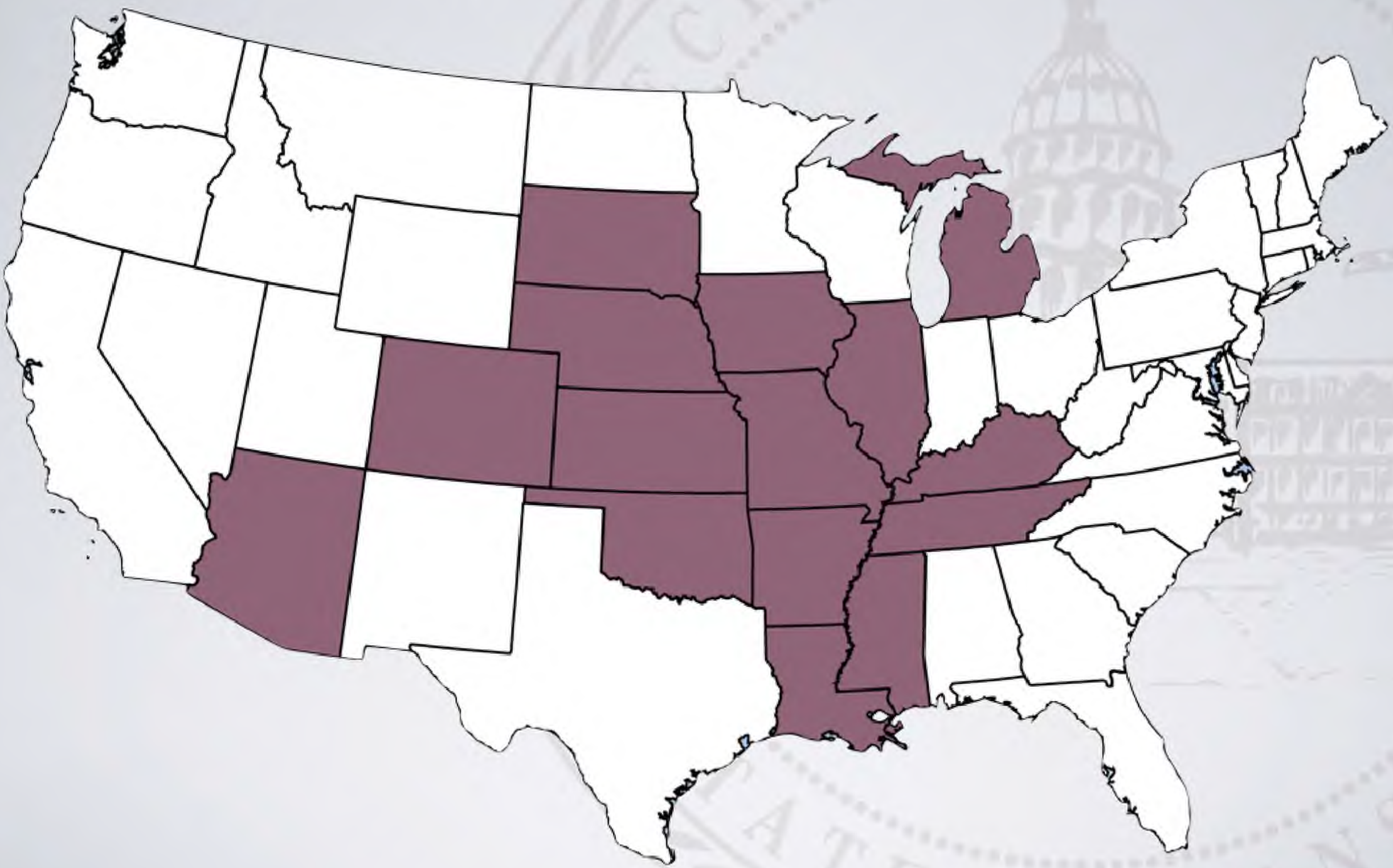
18-F-1517//1275

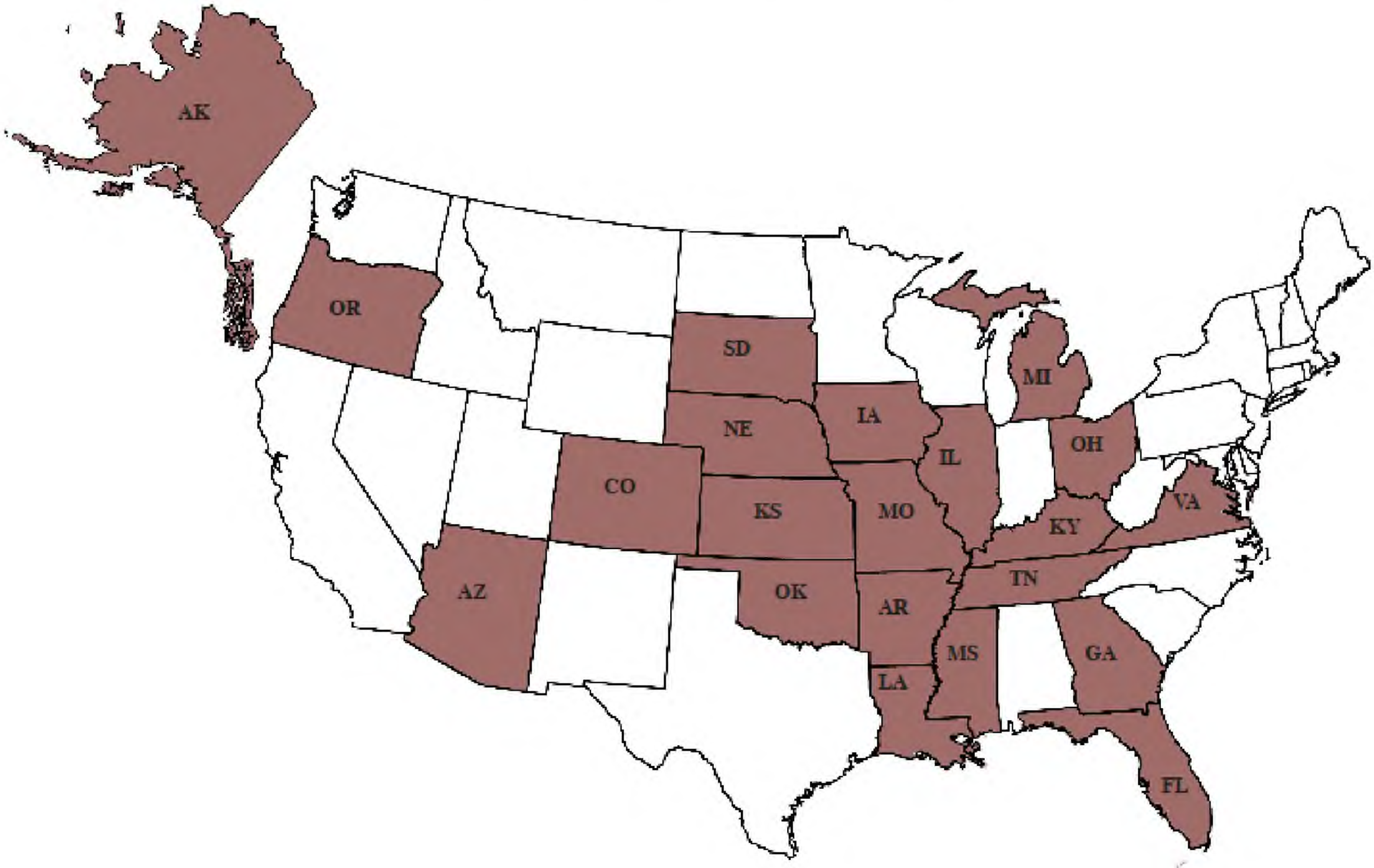
Participants in 2005



18-F-1517//1276

Participants in 2012





2013 Interstate Crosscheck

Participating states as of Jan. 10, 2013

18-F-1517//1278

2012 Crosscheck Program—Number of Records Compared

Arizona	3,545,891	Michigan	7,337,846
Arkansas	1,528,458	Mississippi	2,002,406
Colorado	3,375,891	Missouri	4,069,576
Illinois	8,248,736	Nebraska	1,129,943
Iowa	2,113,199	Oklahoma	2,000,767
Kansas	1,702,495	South Dakota	560,147
Kentucky	1,303,684	Tennessee	3,468,503
Louisiana	2,860,281		

Total Records: 45,247,823

18-F-1517//1279

Interstate Crosscheck Data Format

Field	Format	Example
Status	A=Active; I=Inactive	A
Date_Generated	YYYY/MM/DD	2010/01/01
First_Name		Bob
Middle_Name		Alan
Last_Name		Jones
Suffix Name		Jr
Date_of_Birth	YYYY/MM/DD	1940/06/16
Voter_ID_Number		123456
Last_4_SSN		7890
Mailing Address	Line 1 Line 2 City State Zip	123 Anywhere St...
County		Allen
Date_of_Registration	YYYY/MM/DD	1970/01/01
Voted_in_2010	Y=did vote; N=did not vote	Y

How does it work?

- Each state pulls data on January 15 each year using prescribed data format
- Upload data to secure FTP site (hosted by Arkansas)
- Kansas IT department pulls data, runs comparison, uploads results to FTP site
- Each state downloads results from FTP site, processes them according to state laws & regulations
- Kansas deletes all other states' data

Kris W. Kobach

First: John
Middle: Q.
Last: Public
DOB: 01/01/1975
SSN: 1234
State: Kansas

First: John
Middle:
Last: Public
DOB: 01/01/1975
SSN: 1234
State: Colorado

Potential match

Grid of Potential Duplicate Voters Within States
by DOB Last Name First Name

2012	AZ	AR	CO	IL	IA	KS	KY	LA	MI	MS	MO	NE	OK	SD	TN
AZ		2,829	24,863	16,014	7,153	3,687	688	2,062	27,617	2,220	7,569	3,306	4,006	2,449	3,614
AR	2,829		4,557	6,950	2,430	2,686	691	5,957	5,085	6,477	11,049	995	7,403	433	7,180
CO	24,863	4,557		19,902	10,850	10,035	1,054	5,065	17,086	3,309	12,498	8,927	8,306	3,937	6,153
IL	16,014	6,950	19,902		31,882	6,311	2,467	5,207	49,260	10,766	39,658	3,803	4,834	1,500	12,469
IA	7,153	2,430	10,850	31,882		4,706	526	1,558	7,019	1,797	11,563	10,954	2,031	4,865	2,806
KS	3,687	2,686	10,035	6,311	4,706		401	1,369	4,461	1,397	31,082	4,196	6,575	905	2,205
KY	688	691	1,054	2,467	526	401		873	2,267	1,085	1,195	233	576	117	1,905
LA	2,062	5,957	5,065	5,207	1,558	1,369	873		6,851	17,744	5,254	810	2,829	277	4,422
MI	27,617	5,085	17,086	49,260	7,019	4,461	2,267	6,851		7,527	12,960	2,416	4,067	1,265	16,956
MS	2,220	6,477	3,309	10,766	1,797	1,397	1,085	17,744	7,527		5,607	780	2,364	305	21,661
MO	7,569	11,049	12,498	39,658	11,563	31,082	1,195	5,254	12,960	5,607		4,244	7,539	1,300	7,804
NE	3,306	995	8,927	3,803	10,954	4,196	233	810	2,416	780	4,244		1,126	2,608	1,108
OK	4,006	7,403	8,306	4,834	2,031	6,575	576	2,829	4,067	2,364	7,539	1,126		402	2,858
SD	2,449	433	3,937	1,500	4,865	905	117	277	1,265	305	1,300	2,608	402		537
TN	3,614	7,180	6,153	12,469	2,806	2,205	1,905	4,422	16,956	21,661	7,804	1,108	2,858	537	
Totals	**108,077**	**64,722**	**136,542**	**211,023**	**100,140**	**80,016**	**14,078**	**60,278**	**164,837**	**83,039**	**159,322**	**45,506**	**54,916**	**20,900**	**91,678**

18-1517-1283

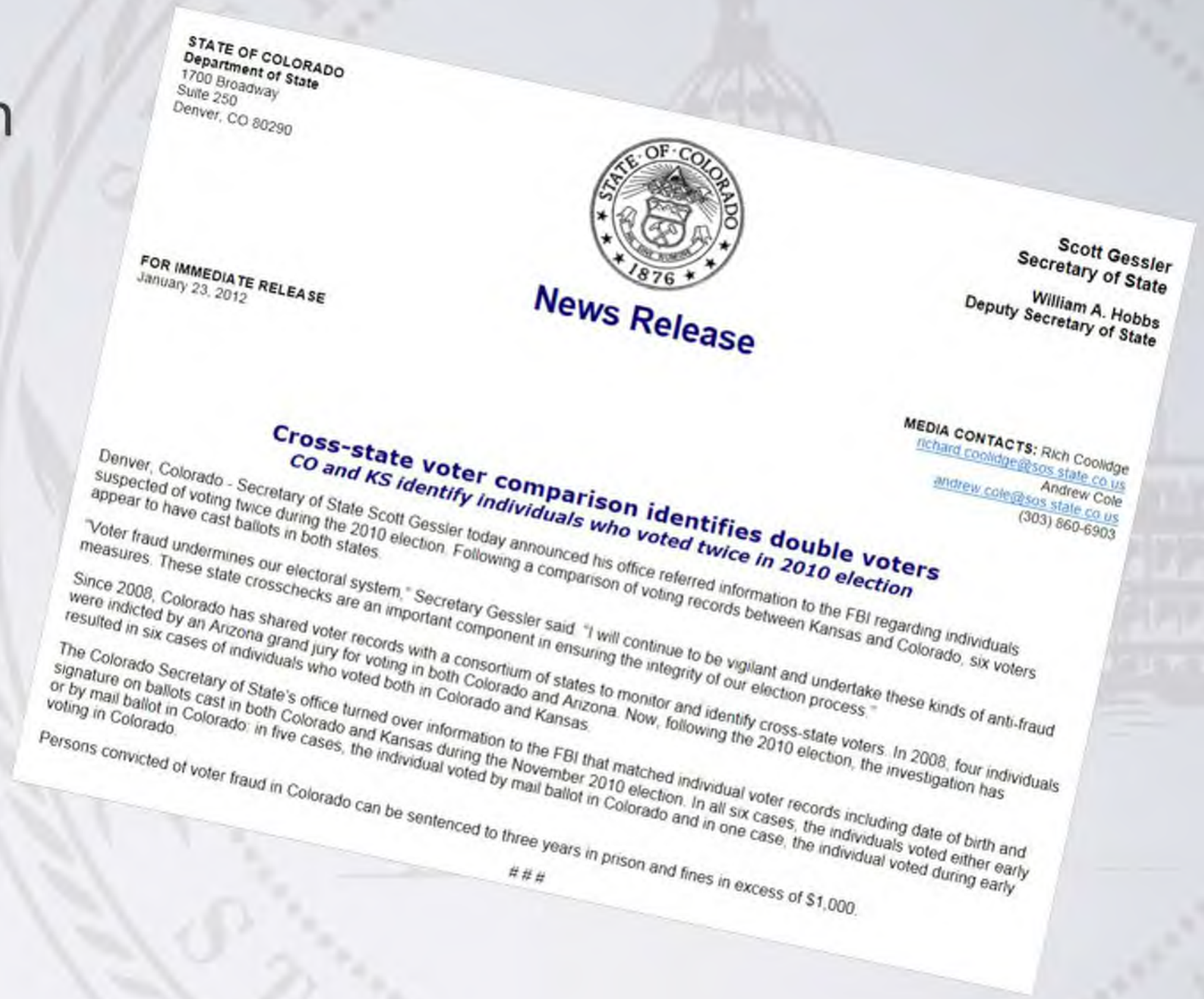
Success in Kansas

Double Votes from 2008 and 2010 Referred to Prosecution Discovered through Interstate Crosscheck Program	
2008	**2010**
Kansas - Kentucky	Kansas – Arkansas (2)
Kansas - Colorado	Kansas – Colorado (5)
Kansas - Kansas	Kansas – Iowa
	Kansas – Louisiana
	Kansas – Nebraska
	Kansas - Oklahoma

Kris W. Kobach

Success in other states - Colorado

- Four individuals indicted for voting in Colorado and Arizona in first year of participation
- Six additional cases of double voting referred to FBI in 2012



STATE OF COLORADO
Department of State
1700 Broadway
Suite 250
Denver, CO 80290

Scott Gessler
Secretary of State

William A. Hobbs
Deputy Secretary of State

FOR IMMEDIATE RELEASE
January 23, 2012

News Release

MEDIA CONTACTS: Rich Coolidge
richard.coolidge@sos.state.co.us
Andrew Cole
andrew.cole@sos.state.co.us
(303) 860-6903

Cross-state voter comparison identifies double voters
CO and KS identify individuals who voted twice in 2010 election

Denver, Colorado - Secretary of State Scott Gessler today announced his office referred information to the FBI regarding individuals suspected of voting twice during the 2010 election. Following a comparison of voting records between Kansas and Colorado, six voters appear to have cast ballots in both states.

"Voter fraud undermines our electoral system," Secretary Gessler said. "I will continue to be vigilant and undertake these kinds of anti-fraud measures. These state crosschecks are an important component in ensuring the integrity of our election process."

Since 2008, Colorado has shared voter records with a consortium of states to monitor and identify cross-state voters. In 2008, four individuals were indicted by an Arizona grand jury for voting in both Colorado and Arizona. Now, following the 2010 election, the investigation has resulted in six cases of individuals who voted both in Colorado and Kansas.

The Colorado Secretary of State's office turned over information to the FBI that matched individual voter records including date of birth and signature on ballots cast in both Colorado and Kansas during the November 2010 election. In all six cases, the individuals voted either early or by mail ballot in Colorado; in five cases, the individual voted by mail ballot in Colorado and in one case, the individual voted during early voting in Colorado.

Persons convicted of voter fraud in Colorado can be sentenced to three years in prison and fines in excess of $1,000.

###

Kris W. Kobach

What does it cost to participate?

$0

How Can a State Join the Crosscheck?

1. Chief State Election Official signs the Memorandum of Understanding (MOU)

2. CSEO assigns two staff members:
   - one election administration person
   - one IT person

3. Staff members will:
   - participate in annual conference call and email
   - pull VR data in January
   - receive cross check results and process
   - instruct local elections officials (respond to requests for addresses, signatures on poll books, etc.)

Contact

Brad Bryant
State Election Director
Kansas Secretary of State's Office
brad.bryant@sos.ks.gov
785-296-4561

18-F-1517//1288

Exhibit 35

The GOP's Stealth War Against Voters

Will an anti-voter-fraud program designed by one of Trump's advisers deny tens of thousands their right to vote in November?

The Crosscheck program is a response to the imaginary menace of mass voter fraud. Mark Makela/Reuters

By Greg Palast
August 24, 2016

When Donald Trump claimed, "the election's going to be rigged," he wasn't entirely wrong. But the threat was not, as Trump warned, from Americans committing the crime of "voting many, many times." What's far more likely to undermine democracy in November is the culmination of a decade-long Republican effort to disenfranchise voters under the guise of battling voter fraud. The latest tool: Election officials in more than two dozen states have compiled lists of citizens whom they allege could be registered in more than one state – thus potentially able to cast multiple ballots – and eligible to be purged from the voter rolls.

The data is processed through a system called the Interstate Voter Registration Crosscheck Program, which is being promoted by a powerful Republican operative, and its lists of potential duplicate voters are kept confidential. But *Rolling Stone* obtained a portion of the list and the names of 1 million targeted voters. According to our analysis, the Crosscheck list disproportionately threatens solid Democratic constituencies: young, black, Hispanic and Asian-American voters – with some of the biggest possible purges underway in Ohio and North Carolina, two crucial swing states with tight Senate races.

RELATED

18-F-1517//1290

2016: First Presidential Election Since Voting Rights Gutted

America will vote for president in a country where it's easier to buy a gun than vote in many states

Like all weapons of vote suppression, Crosscheck is a response to the imaginary menace of mass voter fraud. In the mid-2000s, after the Florida-recount debacle, the Bush administration launched a five-year investigation into the allegedly rampant crime but found scant evidence of wrongdoing. Still, the GOP has perpetuated the myth in every national election since. Recently, North Carolina Board of Elections chief Kim Strach testified to her legislature that 35,750 voters are "registered in North Carolina and another state and voted in both in the 2012 general election." [Editor's note: This quote was taken from the power point that accompanied Strach's testimony. In a subsequent letter, she informed us that during her presentation she "stressed that we were not suggesting that 35,750 voters had committed any type of fraud. My testimony was that the data we received from the Crosscheck Program showed that in the 2012 general election, there were 35,750 people who voted in North Carolina whose first and last names and dates of birth matched persons who voted in the same election in another state."] Yet despite hiring an ex-FBI agent to lead the hunt, the state has charged exactly zero double voters from the Crosscheck list. Nevertheless, tens of thousands face the loss of their ability to vote – all for the sake of preventing a crime that rarely happens. So far, Crosscheck has tagged an astonishing 7.2 million suspects, yet we found no more than four perpetrators who have been charged with double voting or deliberate double registration.

On its surface, Crosscheck seems quite reasonable. Twenty-eight participating states share their voter lists and, in the name of dispassionate, race-blind Big Data, seek to ensure the rolls are up to date. To make sure the system finds suspect voters, Crosscheck

supposedly matches first, middle and last name, plus birth date, and provides the last four digits of a Social Security number for additional verification.

In reality, however, there have been signs that the program doesn't operate as advertised. Some states have dropped out of Crosscheck, citing problems with its methodology, as Oregon's secretary of state recently explained: "We left [Crosscheck] because the data we received was unreliable."

In our effort to report on the program, we contacted every state for their Crosscheck list. But because voting twice is a felony, state after state told us their lists of suspects were part of a criminal investigation and, as such, confidential. Then we got a break. A clerk in Virginia sent us its Crosscheck list of suspects, which a letter from the state later said was done "in error."

The Virginia list was a revelation. In all, 342,556 names were listed as apparently registered to vote in both Virginia and another state as of January 2014. Thirteen percent of the people on the Crosscheck list, already flagged as inactive voters, were almost immediately removed, meaning a stunning 41,637 names were "canceled" from voter rolls, most of them just before Election Day.

We were able to obtain more lists – Georgia and Washington state, the total number of voters adding up to more than 1 million matches – and Crosscheck's results seemed at best deeply flawed. We found that one-fourth of the names on the list actually lacked a middle-name match. The system can also mistakenly identify fathers and sons as the same voter, ignoring designations of Jr. and Sr. A whole lot of people named "James Brown" are suspected of voting or registering twice, 357 of them in Georgia alone. But according to Crosscheck, James Willie Brown is supposed to be the

18-F-1517//1292

same voter as James Arthur Brown. James Clifford Brown is allegedly the same voter as James Lynn Brown.

And those promised birth dates and Social Security numbers? The Crosscheck instruction manual says that "Social Security numbers are included for verification; the numbers might or might not match" – which leaves a crucial step in the identification process up to the states. Social Security numbers weren't even included in the state lists we obtained.

We had Mark Swedlund, a database expert whose clients include eBay and American Express, look at the data from Georgia and Virginia, and he was shocked by Crosscheck's "childish methodology." He added, "God forbid your name is Garcia, of which there are 858,000 in the U.S., and your first name is Joseph or Jose. You're probably suspected of voting in 27 states."

Swedlund's statistical analysis found that African-American, Latino and Asian names predominate, a simple result of the Crosscheck matching process, which spews out little more than a bunch of common names. No surprise: The U.S. Census data shows that minorities are overrepresented in 85 of 100 of the most common last names. If your name is Washington, there's an 89 percent chance you're African-American. If your last name is Hernandez, there's a 94 percent chance you're Hispanic. If your name is Kim, there's a 95 percent chance you're Asian.

The Crosscheck program, started by Kris Kobach, has spread to over two dozen states, tagging more than 7 million voters as possibly suspect. Christopher Smith/Washington Post/Getty

This inherent bias results in an astonishing one in six Hispanics, one in seven Asian-Americans and one in nine African-Americans in Crosscheck states landing on the list. Was the program designed to target voters of color? "I'm a data guy," Swedlund says. "I can't tell you what the intent was. I can only tell you what the

18-F-1517//1293

outcome is. And the outcome is discriminatory against minorities."

Every voter that the state marks as a legitimate match receives a postcard that is colorless and covered with minuscule text. The voter must verify his or her address and mail it back to their secretary of state. Fail to return the postcard and the process of taking your name off the voter rolls begins.

This postcard game amplifies Crosscheck's built-in racial bias. According to the Census Bureau, white voters are 21 percent more likely than blacks or Hispanics to respond to their official requests; homeowners are 32 percent more likely to respond than renters; and the young are 74 percent less likely than the old to respond. Those on the move – students and the poor, who often shift apartments while hunting for work – will likely not get the mail in the first place.

At this point, there's no way to know how each state plans to move forward. If Virginia's 13 percent is any indication, almost 1 million Americans will have their right to vote challenged. Our analysis suggests that winding up on the Crosscheck list is hardly proof that an individual is registered in more than one state. Based on the data, the program – whether by design or misapplication – could save the GOP from impending electoral annihilation. And not surprisingly, almost all Crosscheck states are Republican-controlled.

The man behind crosscheck is Kansas Secretary of State Kris Kobach, a Yale-educated former law professor. After 9/11, U.S. Attorney General John Ashcroft tasked Kobach with creating a system to track foreign travelers. (It was later shut down over concerns about racial profiling.) He is best known as the author of Arizona's "Driving While Brown Law," which allowed cops to pull over drivers and ask for proof of their legal status. He co-wrote the ultraconservative 2016 RNC

18-F-1517//1294

party platform, working in a recommendation that Crosscheck be adopted by every state in the Union. He's also the Trump adviser who came up with a proposal to force Mexico into paying for Trump's wall.

In January 2013, Kobach addressed a gathering of the National Association of State Election Directors about combating an epidemic of ballot-stuffing across the country. He announced that Crosscheck had already uncovered 697,537 "potential duplicate voters" in 15 states, and that the state of Kansas was prepared to cover the cost of compiling a nationwide list. That was enough to persuade 13 more states to hand over their voter files to Kobach's office.

In battleground-state Ohio, Republican Secretary of State John Husted's Crosscheck has flagged close to half a million voters. In Dayton, we tracked down several of the suspects on our lists. Hot spots of "potential duplicate" voters, we couldn't help but notice, were in neighborhoods where the streets are pocked with rundown houses and boarded storefronts. On Otterbein Avenue, I met Donald Webster, who, like most in his neighborhood, is African-American.

Crosscheck lists him registered in Ohio as Donald Alexander Webster Jr., while registered a second time as Donald *Eugene*Webster (no "Jr.") in Charlottesville, Virginia. Webster says he's never been a "Eugene" and has never been to Charlottesville. I explained that both he and his Virginia doppelgänger were subject to losing their ability to vote.

"How low can they go?" he asked. "I mean, how can they do that?"

I put his question to Robert Fitrakis, a voting-rights attorney who examined our Crosscheck data. I showed him Donald Webster's listing – and page after page of Ohio voters. Fitrakis says that the Ohio secretary of state's enthusiasm for Crosscheck fits a pattern: "He

doesn't want to match middle names, because he doesn't want real matches. They're targeting people with clearly defined ethnic names that typically vote for the Democratic Party. He wants to win Ohio the only way he knows how – by taking away the rights of citizens to vote."

Kobach refused to speak for this story. So I went to Newton, Kansas, where he was headlining an ice-cream-social fundraiser in a public park. I approached Kobach with the Crosscheck list he had refused me, and asked, "Why are these lists so secret?"

RELATED
Watch John Oliver's Takedown of Voter ID Laws
"It's just one of those things that white people are more likely to have. Like a sunburn. Or an Oscar nomination," host says of IDs

"They aren't," Kobach answered, contradicting what his attorney had told me.

I pointed to a random match on the Crosscheck list and asked him why it identified James *Evans* Johnson as the same voter as James P. Johnson.

Kobach denied the name could be on the list. "Our system would not yield this match," he said. (And according to the rules of his program, it shouldn't have.)

"This is the list you gave [Virginia], and they knocked off 41,000 voters," I said.

"That is false!" he said, as he hurried away. "You know why? Federal law prohibits that."

Kobach is correct that federal regulation typically would complicate such a sweeping purge, but somehow tens of thousands of voters in Virginia got knocked off the rolls anyway.

Kobach's Crosscheck purge machinery was in operation well before Trump arrived on the political scene – and will continue for elections to come. Low voter turnout of any kind traditionally favors the GOP, and this is the party's long game to keep the rolls free of young people, minorities and the poor. Santiago Juarez of New Mexico, an attorney who has done work for the League of United Latin American Citizens, has spent years signing up Hispanic voters in the face of systemic efforts to suppress their vote. He scoffed at the idea of a massive conspiracy among Latinos to vote in two states. "Hell," he said, "you can't get people to vote once, let alone twice."

18-F-1517//1297

Exhibit 36

THE U.S. DIGITAL SERVICE

Report to Congress – December 2016

18-F-1517//1299

Table of Contents

18-F-1517//1300

Section 1

Introduction

18-F-1517//1301

In August 2014, the United States Digital Service (USDS) was created to improve the Federal Government's most important public-facing digital services. USDS is a collaboration between some of the country's top technical talent and the government's brightest civil servants, who work in partnership to apply private sector best practices to our digital services.

Initially, USDS' small team of technologists planned to focus on three projects. Additional funding and the support of Congress for the Information and Technology Oversight and Reform (ITOR) Fund in the 2015 and 2016 Fiscal Year appropriations bills allowed USDS to invest in a greater number of high-priority projects, detailed in this report. Of the $30M appropriated in the 2016 fiscal year, $14M was apportioned to USDS to support its operations, with the balance of the $30M supporting other IT oversight and reform activities. At its creation, USDS was administratively placed within the Office of the Federal CIO. After more than two years of operations, however, the Office of Management and Budget (OMB) has decided to move the Administrator of USDS to directly report to the Deputy Director of Management (DDM).

USDS staff in OMB work alongside agency Digital Service team staff to support high-priority projects in agencies including the Departments of Veterans Affairs, State, Education, Homeland Security, Health and Human Services, Defense, the Internal Revenue Service, and the Small Business Administration.

The central focus of USDS is on the measurable improvement of the performance and cost-effectiveness of important, public-facing Federal Government digital services – via the application of modern technology best practices. To execute this mission, USDS conducts hands-on engagements with agencies. A summary of USDS' most impactful engagements is provided in Section 2.

In support of its core mission of improving the performance and cost-effectiveness of important government digital services, the USDS engages in three additional activities:

- **Rethink how we build and buy digital services.** USDS is working on modernizing procurement processes and practices for the modern digital era. Our partners in the IT contracting community are a critical element of modernizing our government, as skilled contractors deliver the majority of the government's digital services.
- **Expand the use of common platforms, services and tools.** USDS is working with agencies to identify and implement shared tools and services to address common technical issues and usability challenges across the Federal Government. One example is building Login.gov, a universal login system that will enable the

18-F-1517//1302

American public to access multiple government agency services with one, streamlined account.

- **Bring top technical talent into public service.** In support of these goals, USDS has recruited and placed over 200 Digital Service Experts, from one of the most competitive industries in the world, to join the government for term-limited tours of duty with the USDS and work with civil servants inside agencies. The long-term goal is to encourage a tradition of public service in the tech industry that will support the ongoing improvement of government digital services.

USDS has developed procedures and criteria for prioritizing projects, which includes obtaining input from OMB's IT Dashboard, agency leadership, and relevant U.S. Government Accountability Office (GAO) reports. To prioritize projects, USDS also uses the following three criteria, which are listed in their order of importance:

(1) What will do the greatest good for the greatest number of people in the greatest need?
(2) How effective and cost-efficient will the USDS investment be?
(3) What potential exists to use or reuse a technological solution across the Federal Government?

Along with its investment in the ITOR Fund, Congress asked USDS to provide a regular update on progress in each of its programs. This report details that progress.

Mikey Dickerson
Administrator, U.S. Digital Service

18-F-1517//1303

Section 2

High Priority Projects

18-F-1517//1304

Priority Project Summary

USDS executes focused, hands-on engagements in which small teams of technical experts embed into existing agency programs, where they accelerate adoption of modern private sector best practices on important projects. These engagements may be proactive or reactive, and can range from two-week diagnostic sprints to in-depth multi-month engagements to dramatically improve a target service.

Typically, USDS is focused on increasing the success rate of a major IT acquisition in an agency. USDS personnel help promote the critical factors underlying successful major IT acquisitions identified by GAO in 2011 and reiterated in 2015 by GAO in its report on "Improving the Management of IT Acquisitions and Operations."

This section details USDS' most impactful projects, including those completed during the 2016 Fiscal Year:

- **Stabilizing and Improving HealthCare.gov (page 9).** In the 2013-2014 Open Enrollment season, a small team of private sector experts helped overhaul, update, and simplify the design and infrastructure of HealthCare.gov, helping eight million Americans sign up for coverage. This success paved the way for the creation of USDS. In the two subsequent open enrollment periods, USDS staff continued to partner with CMS staff and contractors to further improve the HealthCare.gov system and services.
- **Modernizing the Immigration System at DHS (page 14).** Since 2014, USDS has been helping USCIS implement private sector best practices on the Electronic Immigration System project. As of September 2016, 25% of immigration transactions applications are processed electronically using the system, including the green card renewal application (I-90), which has a 92% user satisfaction rate.
- **Streamlining VA Disability Claim Processing (page 20).** Over the summer of 2016, the USDS team at VA helped launch Caseflow Certification, a tool to improve paperless appeals processing by detecting if required documentation has been added before an appeal can move forward. This simple check helps reduce preventable errors and avoidable delays caused by disjointed, manual processing. As of September 2016, approximately 87% of all paperless appeals are certified using the tool.
- **Simplifying Veteran-facing Services with Vets.gov (page 26).** USDS is working with leaders across VA to build Vets.gov, a simple, easy-to-use site that consolidates information for Veterans. Over the summer, the USDS team helped VA launch a new digital application for healthcare built with feedback from

18-F-1517//1305

Veterans. Previously, less than 10 percent of applicants applied online. Since the launch of the new healthcare application, daily online applications have increased from 62 per day to more than 500 per day.

- **Providing Secure Access to IRS Taxpayer Information (page 31).** USDS helped IRS introduce Secure Access in June 2016, a user verification process that relies on strong identity proofing and two-factor authentication to protect users' sensitive tax records. Secure Access ensures that users have convenient, real-time access to their transcripts while protecting taxpayer information from automated fraudulent attacks. As of September 2016, taxpayers have accessed 2.7 million tax records using the Secure Access process.
- **Improving the Visa Processing System at Department of State (page 37).** USDS is assisting State to implement improvements in the Consolidated Consular Database, on which many Visa processing applications depend. USDS helped State adopt modern engineering best practices, and is helping State develop tools to communicate case status to applicants, which is the primary reason for many of the 9,000 phone calls the National Visa Center receives per day.
- **Helping CMS Implement Congressionally Mandated Medicare Payment Changes (page 41).** Implementation of the Medicare Access and Chip Reauthorization Act of 2015 (MACRA) will change the way Medicare pays doctors for services rendered to Medicare patients. USDS is helping CMS use modern best practices to ensure the transition from the current payment program to the new system is simple, clear and effective.
- **Reducing Inefficiency in the Refugee Admission Process (page 44).** Each year, the United States admits tens of thousands of refugees using a rigorous approval process. Previously, DHS officers had to approve refugee registration forms using an ink approval stamp in the field where the refugee file was physically located. USDS helped DHS and State implement a "digital stamp," removing an unnecessary processing delay of 2 to 8 weeks for thousands of cases.
- **Helping Students Make More Informed College Choices at Department of Education (page 49).** USDS, along with 18F, helped the Department of Education launch the College Scorecard to help students make more informed decisions about college selection. Millions of students have already benefited from this data, the most comprehensive and reliable ever published on employment outcomes and success in repaying student loans. Additionally, more than a dozen organizations have built new tools using the data.
- **Modernizing the Department of Defense Travel System (page 55).** The USDS team at DoD (Defense Digital Service) is helping implement a new commercial

18-F-1517//1306

tool to better manage the $3.5 billion of travel handled through the Defense Travel System each year.

- **Identifying Security Vulnerabilities in Department of Defense Websites (page 59).** To strengthen data security at DoD, the USDS team at DoD (Defense Digital Service) launched "Hack the Pentagon," the first bug bounty program in the history of the Federal Government. Adopting this private sector best practice led to the resolution of 138 previously unidentified vulnerabilities and cost $150,000, compared to the $1 million DoD estimates contracting an outside firm to do a similar audit would have cost.

Additional detail on each of these projects is provided in the chapters below.

18-F-1517//1307

Stabilizing and Improving HealthCare.gov

The Challenge

As required by the Affordable Care Act, HealthCare.gov is the Federal website that facilitates purchase of private health insurance for consumers who reside in states that did not establish health insurance marketplaces. HealthCare.gov supports the Federal Health Insurance Marketplace (Marketplace), providing citizens with the ability to compare, shop for, and enroll in affordable healthcare plans.

HealthCare.gov launched in October 2013, and encountered serious technical challenges which prevented many people from using the service.

Project Impact Summary

- A team of private sector engineers and product managers joined CMS staff and contractors to identify and solve website operation problems. By March 2014, over 8 million Americans had successfully signed up for health insurance and the site was stable.
- In the two subsequent open enrollment periods, USDS staff continued to partner with CMS to improve the HealthCare.gov system and services. USDS staff helped CMS implement several private sector best practices including performance tracking of the system and application process, building an improved identity management solution with an uptime of 99.99%, increasing the conversion rate in the new application workflow from 55% to 85%, and building new systems with industry standard open source software.

The Solution

Over the three month period following the launch, a team of engineers and product managers from the private sector joined with CMS staff and existing contractor teams to troubleshoot the service. Working around the clock, this "tech surge" team systematically identified and solved problems with the service by following industry best practices in site reliability and product management. By March 2014, the end of the Marketplace's first open enrollment period, over 8 million Americans had successfully signed up for health insurance.

The HealthCare.gov turn-around demonstrated the enormous potential of empowering small teams of America's brightest digital talent to apply modern technology best

18-F-1517//1308

practices to Federal Government projects. In August 2014, the White House established the U.S. Digital Service (USDS) to apply this technique to a greater number of projects. Mikey Dickerson, a site reliability engineer on the HealthCare.gov team, was appointed the USDS Administrator.

In the two subsequent open enrollment periods (ending February 2015 and January 2016), USDS engineers, product managers and designers partnered with CMS staff to continue to improve HealthCare.gov systems and processes used to deliver the service.

For example, contractors from multiple companies along with CMS staff improved coordination in the Healtchare.gov operations center by embracing a "one-team" mentality with fewer process restrictions, which has improved the ability of this team to troubleshoot issues and make important decisions quickly. The team also implemented application monitoring to track performance.

Additionally, USDS supported several smaller teams working on components of HealthCare.gov which adopted agile and iterative development processes, allowing them to quickly deliver functioning software. In one such case, a small team built and launched the Scalable Login System (SLS), a replacement for HealthCare.gov's previous identity management solution. SLS has proven to be vastly more stable and efficient since it was created specifically for use by Marketplace consumers.

Additionally, CMS launched a simpler and more efficient application for healthcare plan enrollment (Marketplace Lite 2.0 App). The conversion rate in the new application workflow stands at around 85%, compared with approximately 55% in the previous system. Finally, CMS with input from the insurer community, built and launched a new set of decision support tools for the window shopping and plan compare tools. These tools allow consumers to search for preferred doctors, prescription drugs, and facilities while shopping for a health plan. This was one of the most requested features from Marketplace consumers over the past several years.

Success Criteria	Status
Transition HealthCare.gov to a scalable login system with an uptime of 99% or greater	Complete. Scalable Login System implemented and users migrated to the system in 2015. Uptime 99.99%
Implement application monitoring.	Complete. Monitoring installed and in use.
Launch the Marketplace Lite 2.0 app	Complete. App launched in 2015, resulting in improved conversion rates.

Milestones

- October 2013: HealthCare.gov launches. "Tech surge" assists with troubleshooting the service.
- March 2014: First open enrollment period closes with 8 million Americans enrolled (5.3 million through HealthCare.gov).
- August 2014: USDS created.
- November 2014: Second open enrollment period begins. USDS team supports Marketplace operations.
- February 2015: Second open enrollment period ends with 11.7 million enrollments (8.8 million through HealthCare.gov). USDS team supports Marketplace operations and assists with the transition from to SLS.
- November 2015: Third open enrollment period begins. USDS team supports Marketplace operations
- January 2016: Third open enrollment period ends with 12.7 million enrollments (9.6 million through HealthCare.gov). USDS support role winds down.

18-F-1517//1310

The Process and Lessons Learned

1. **Install application monitoring.** At initial launch of HealthCare.gov, there was no end-to-end monitoring of the production system, making identification, prioritization and diagnosis of errors very challenging. One of the first actions the "tech surge" team took was to recommend the addition of an application monitoring tool, which has remained an important resource for the team to identify issues as they occur.

2. **Facilitate open and direct communication between technical contributors.** HealthCare.gov has many components, many of which were created by different companies hired by CMS. Problems with the integration of these components was a source of many errors in the initial launch. The most effective solution was to bring individual technical contributors from these various teams to a single location where problems could be discussed openly, solutions could be explored, and assignments could be made. Additionally, all staff and contractors working on aspects of HealthCare.gov began to use a collaboration tool to communicate more effectively.

3. **Deploy in a flexible hosting environment.** Traffic on HealthCare.gov is highly variable. Near the end of an enrollment period, for example, the number of visitors can increase by an order of magnitude.

   Several of the newer components of HealthCare.gov are deployed in a flexible cloud hosting environment (including SLS and the Marketplace Lite App 2.0 described above). CMS has experienced high availability and increased development speeds with this approach, and is seeking to use this approach for more of its components.

4. **Build services using agile and iterative processes.** CMS has had success using small teams to incrementally deliver enhanced functionality based on an evolving understanding of user needs. For example, the Marketplace Lite App 2.0 continues to be iteratively improved based on user feedback and metrics.

5. **Choose a modern technology stack.** The Scalable Login System was built with industry standard open source software components commonly used by the private sector. The service is deployed in the public commercial cloud. These decisions enabled the team to build the service at a lower cost.

18-F-1517//1311

Modernizing the Immigration System at DHS

The Challenge

Every year, the Department of Homeland Security's U.S. Citizenship and Immigration Services (USCIS) processes millions of immigration requests. This system is mostly paper-based, consists of multiple forms, and results in long waiting periods for applicants who have little visibility into the status of their applications.

USCIS wanted to modernize the process. They wanted a streamlined experience that would allow applicants to identify which form was meant for their specific situation, and enable adjudicators to process applications more efficiently and effectively than on paper.

To achieve this goal, USCIS began a five-year engagement with a technology vendor to create the Electronic Immigration System (ELIS). The project ran into a host of issues: the project scope was too large, the proprietary technology adopted was too complex and inflexible, and releases happened years after the project began. The agency was heavily reliant on specific vendors and proprietary technologies that proved costly and difficult to customize to address USCIS' product requirements.

ELIS fell short of expectations and didn't meet user needs – so USCIS made the hard but correct decision to restart the project using a new management style and a new technical approach that took key plays from private industry.

In 2014, members of the USDS joined the USCIS team to help the agency implement these changes, and the USDS has provided ongoing support to the agency since then.

Project Impact Summary

- Every year, USCIS processes millions of immigration requests. Its multi-year project to modernize this process (the ELIS project) ran into a host of issues common in Federal Government IT projects, leading USCIS to restart the project.
- In 2014, USDS staff engineers, designers and product managers began working with USCIS to help it implement private sector IT management best practices including agile software development and continuous integration.
- In March 2015, following a November 2014 soft launch, USDS supported USCIS with the release of online filing and adjudication of the Form I-90, the application to replace permanent resident cards. 92% of online I-90 filers (renewing or replacing their green cards) reported being satisfied with the experience.

18-F-1517//1312

- In February 2015, USCIS partnered with 18F, private contractors, and USDS to launch myUSCIS, a new service to help applications and their representatives better navigate the immigration process.
- The Immigrant Fee payment launched in August 2015, enabling over 1.1 million applicants to make fee payments digitally.
- USCIS has adopted deployment approaches that allow it to release improvements to ELIS weekly, compared to the quarterly release schedule the project followed previously.
- Today, 25% of immigration applications are processed electronically and USDS continues to work with USCIS to increase this percentage.

The Solution

In restarting the project, USCIS leadership changed the way they did business.

The team embraced an agile, iterative style of product development that allowed the agency to design, build and deploy functionality more quickly to respond to user needs. While the previous project had taken years before an initial launch, the new approach led to a beta release just one year after development began. Agency staff are now heavily involved in the day-to-day development effort, running stand-up meetings and increasing visibility across the team. Seasoned USDS product managers, engineers and designers partnered with the USCIS team to integrate these modern digital service practices.

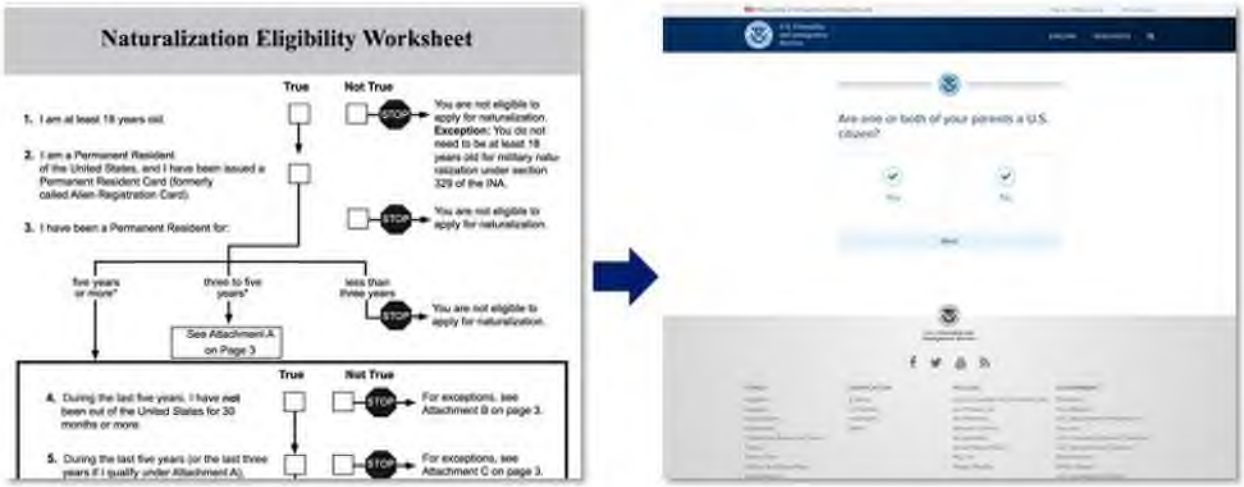
In order for the team to effectively support this agile development style, USCIS had to change its approach to contracting. They engaged with multiple vendors instead of using one large contract with a single vendor. The teams worked together to deliver features, build and maintain the infrastructure for the service, and enable the continuous integration of new improvements into the production system. The contracts are designed to support frequent prototyping, refining of product requirements, and delivery of working software. Most of them give USCIS the flexibility to ramp up or down the number of development teams from each vendor based on that vendor's performance.

USCIS also conducted deep research on their customers that led them to re-imagine the end-to-end immigrant experience well beyond the core actions of filing and processing requests. They began to redesign the immigrant experience around people, not form numbers.

In partnership with 18F and private contractors, USCIS brought this vision to life by launching myUSCIS, a new service built to help applicants and their representatives.

18-F-1517//1313

myUSCIS allows visitors to determine which immigration options are available to them, with a search-driven, plain-language knowledge base of direct answers to common immigration questions. It also now allows immigrants to apply for naturalization, make fee payments, provide supporting evidence, and look up their case status online.



Finally, USCIS technical leaders also made important changes to the architecture of ELIS. The development team has adopted many modern software development practices drawn from the private sector, including the use of open source software components, flexible deployment environments, and real-time monitoring. The team also continuously integrates changes to the system, using modern deployment and testing processes and tools. USCIS is implementing the "DevOps" model, in which there is no separation between development and operations teams.

These improvements in software development practices, design and system architecture are making it easier for users to interact with our immigration system. The team has hit several important milestones, including the release of online filing and adjudication of the Form I-90 (application to replace permanent resident card). USCIS has also begun to electronically process applications for naturalization. USCIS will continue to bring more parts of the immigration process into the new digital system and improve its processes around design, high-quality delivery, and system monitoring and response.

USDS will remain involved with the project to assist with delivery, design and operations.

18-F-1517//1314

Success Criteria	Status
Increased percentage of immigration applications processed electronically	In progress. 25% of immigration applications are now processed electronically
Increased customer satisfaction rating over time	In progress. 92% of online I-90 filers (renewing or replacing their green cards) reported being satisfied with the experience.
Increase frequency of ELIS releases	Complete. ELIS releases new code weekly, up from previous quarterly releases

Milestones

- July 2014: A "pilot" USDS engagement prior to its official launch in August began with a "Discovery Sprint" focused on ELIS
- November 2014: ELIS2 I-90 Three-Day "Soft" Launch
- March 2015: ELIS2 I-90 Full Launch
- August 2015: Immigrant Fee payment launched
- April 2016: ELIS2 Naturalization Pre-processing Go-live Date

The Process and Lessons Learned

1. **Understand what people need.** The USDS team helped USCIS implement a user-centered design process to ensure that the delivery team understood what people need the service to offer. USDS coordinated and led visits to field offices and the National Benefit Center to conduct direct observation of application processing, giving insight into users' needs and experiences. This user research informed the design of the system. The team further refined these designs by getting adjudicator feedback on simple mockups of functionality, and testing early versions of the system with adjudicators.

2. **Build services using agile and iterative practices.** In the new system, USCIS chose two high-volume services and focused on rapidly digitizing them using an

18-F-1517//1315

agile development process. The Form I-90 application to replace a permanent resident card was first launched in November 2014, and USCIS Immigrant Fee Payment launched in August 2015. These services were rolled out in an incremental manner, and teams continue to deliver bug fixes and enhancements on a weekly basis. The teams collect feedback from end users and engage in regular usability testing to identify opportunities to improve efficiency and inform development of future product lines.

3. **Structure budgets and contracts to support delivery.** The USCIS CIO spearheaded an innovative contracting approach, which replaced a single large vendor with multiple contractors working together and competing for business. Each contractor provides cross-functional development teams that participate in the iterative product development process, working with federal product owners and project managers. Each vendor is evaluated based on its ability to rapidly deliver working software.

4. **Deploy services in a flexible hosting infrastructure.** USCIS chose to use a "public cloud" infrastructure service provider to host the service. This choice makes it easy and cost-effective for the team to provision, configure and adjust virtual computing resources as needed.

5. **Identify and empower product owners.** USCIS centralized the product development effort in its Office of Transformation Coordination, led by a single executive. This executive has identified product owners for each business line, who are each empowered and responsible for the digitization of that business line's product. Each product owner can prioritize work, advocate for users, and accept delivery of features from the contractor staff. USDS provided training and support to these product owners, and advocated for the creation of this product management structure.

6. **Implement robust monitoring and incident response.** USDS led an initiative to create a rapid response procedure for troubleshooting major incidents such as service outages. This procedure involves identifying "incident commanders" who are empowered to make quick decisions and the use of an alerting tool (currently PagerDuty) to coordinate incident response.

7. **Use "soft launches" to help identify issues prior to full release.** The USCIS team has incremental releases built into its process. For example, the ELIS2 external interface was opened to accept I-90 applications for 72 hours in November 2014. The applications received in this "soft launch" window were then processed using the new system, allowing USCIS to complete an end-to-end test

18-F-1517//1316

of the service with real data. The results of this test were used to refine the service prior to its full launch in February 2015.

8. **Rely on automated tests to increase development speed.** Good automated test coverage allows the team to verifiably demonstrate the system is working as intended, and speeds the development process by providing instant and reliable feedback to developers about how changes they have made to the system have impacted existing functionality. Working together, USDS engineers and contractor teams have increased the use of automated unit and integration tests.

18-F-1517//1317

Streamlining VA Disability Claim Processing

The Challenge

When a veteran has a disease or injury related to service, he or she may file a claim for disability compensation for the service-connected disease or injury. These claims are filed with the Department of Veterans Affairs (VA) and can result in a grant, partial grant, or denial. If a veteran is unsatisfied with the outcome of his or her claim, he or she may file an appeal. Since 1996, the appeal rate has averaged 11 to 12 percent of all claims decisions.

Between FY 2010 and FY 2015, the Veterans Benefits Administration (VBA) completed more than 1 million claims annually, with nearly 1.4 million claims completed in FY 2015. As VA has increased claims decision output over the past 5 years, appeals volume has grown proportionately. Today, there are more than 450,000 pending appeals, and this number is expected to grow to 1 million by 2025 without legislative reform.

The current IT system used to track and process appeals at the Board of Veterans' Appeals and across the VA is more than 20 years old and is built on outdated infrastructure. It powers a variety of workflows essential to the appeals process across VA, but is difficult to use and hard to update, and it is straining under the increased volume of appeals. With such a large volume of paperless cases that travel across jurisdictions within the VA, from the local regional office level to the Board and back again, the VA needed an updated IT solution to ensure full and seamless accountability of all appeals as well as data integrity through integration of systems, increased automation, and reduced manual processes. VA recognized that the processes and technology underpinning the appeals system needed improvements, and began the Appeals Modernization initiative in 2014.

18-F-1517//1318

A screenshot from the current VA IT system used to track and process appeals

Project Impact Summary

- The legacy IT system used to track and process appeals at the Board of Veterans' Appeals is more than 20 years old and is built on an outdated infrastructure.
- A team of three Digital Service at VA staff worked with the VBA beginning in June 2015 to design and implement a new Caseflow Certification tool to provide the Board with all of the information it needs to process an appeal.
- Digital Service at VA developed a script that discovered 2,172 appeals that had been incorrectly categorized and were in limbo. Without this script, appeals in this state may have remained unprocessed for an indefinite period of time.
- As of September 2016, approximately 87.3% of all paperless appeals are now certified using Caseflow Certification. The new tool was successfully rolled out as certification volume increased 34.1% from the year ago period.
- As of September 2016, Caseflow Certification handles 5,000+ certifications per month.

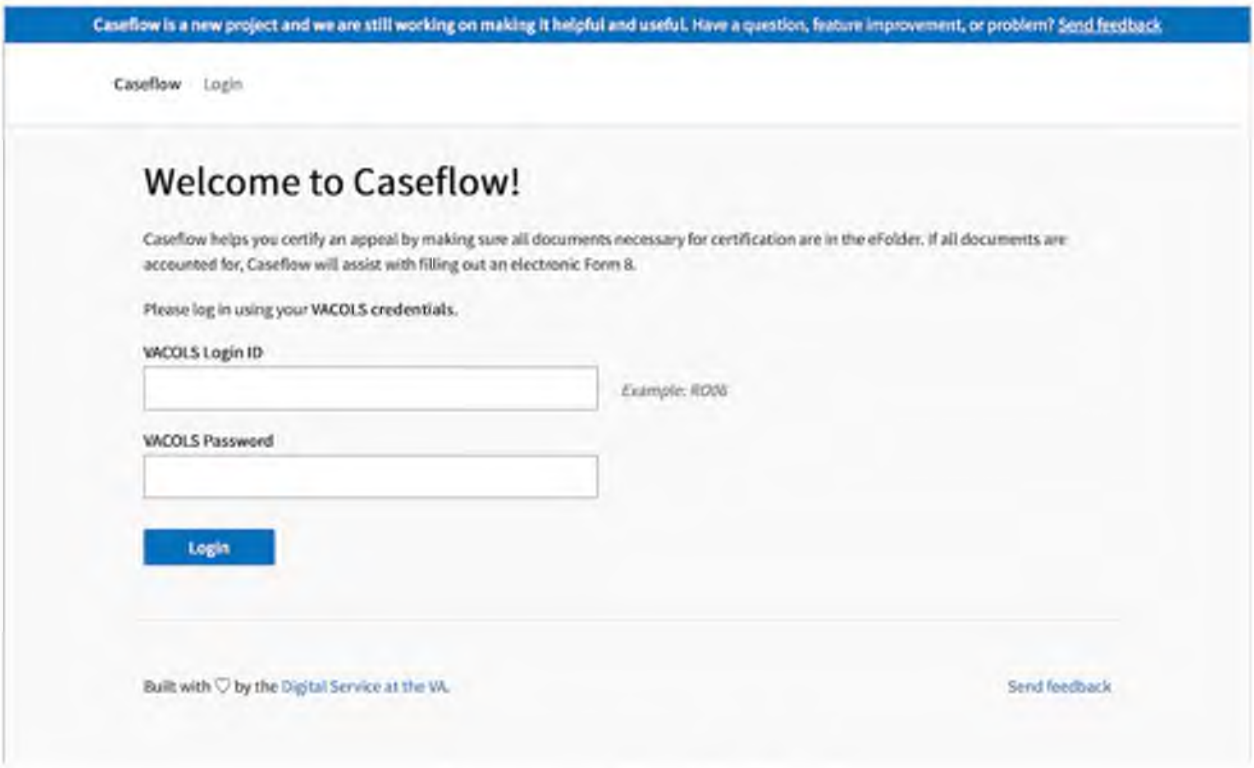
- Digital Service at VA awarded an agile contract on T4NG in September 2016, using a coding exercise to determine contractors' capabilities.
- With a new contract in place, the Caseflow team is growing to 30, including nine Digital Service at VA staff.
- In October 2016, Digital Service at VA began rolling out eFolder Express to the Office of General Counsel and the Records Management Center to improve the efficiency with which appeal documents can be retrieved, including for Privacy Act requests.

The Solution

The U.S. Digital Service at VA (DSVA) – the U.S. Digital Service's first agency digital service team – has worked closely with the Board of Veterans' Appeals to develop a new system that tracks and processes paperless appeals, called Caseflow. This system will have many user-facing web applications that map to existing workflows in the appeals process such as Certification, Activation, Review, and Dispatch. The team is using an iterative approach that will gradually replace small portions of the older system as new components are created, minimizing any disruption to existing business processes. In addition, the USDS modular approach enables quick updates and changes to Caseflow should there be any changes in legislation, regulation, or VA policy.

Caseflow Certification, released nationwide in April 2016, is the first component of the modernized system to be deployed. Caseflow Certification is a tool for VA employees to ensure that the Board has all of the information it needs to process the appeal, and that the data in the claims system — known as the Veterans Benefits Management System (VBMS) — matches the data in the appeals system, known as the Veteran Appeals Control and Locator System (VACOLS). Because many appeals that arrived at the Board contained manual data errors or were incomplete, providing VA employees at regional offices better tools to verify and reconcile key information using automated steps has been critical to optimizing accuracy and efficiency, and ensuring data integrity through system integration. Caseflow Certification also provides a simplified way for staff to generate a VA Form 8 – the Certification of Appeal – which is a required step in the appeal process. The tool automatically populates many fields of this form based on data in the system, reducing manual data entry to just a handful of questions. It also allows staff to file the form in the claims system with a single click, rather than requiring users to switch browser windows, navigate to the veteran's case folder, and manually upload the form.

18-F-1517//1320



A screenshot from Caseflow.

In addition to the user-facing component, Caseflow Certification allowed the DSVA team to develop and run an important script that helps the Board identify pending appeals that may have been incorrectly categorized as paper transfers, when in fact the appeals were paperless. Without this step, the Board could be left waiting for a physical appeal to arrive at its facility when in fact none exists. Without the Caseflow Certification tool, appeals in this state could have remained unprocessed for an indefinite period. The DSVA team discovered 2,172 appeals in this state by running the script. This enabled the VA to proceed with processing these Veterans' appeals, and to take preventative measures to avoid the problem in the future. The DSVA continues to monitor the data to detect appeals that could end up in this state again.

As of September 2016, approximately 87.3% of all paperless appeals are now certified using Caseflow. The remaining appeals are certified using the legacy process, and represent edge case scenarios. The DSVA is working to incrementally improve the Caseflow Certification tool so it can be used in more of these uncommon scenarios. Throughout the rollout, DSVA promptly responded to feedback and issues reported by VA employees.

Success Criteria	Status
All appeals are certified using Caseflow	In progress. At present, 87.3% of paperless appeals are processed using Caseflow.

Milestones

- June 15, 2015: DSVA engagement began
- July-August 2015: Discovery Sprint
- March-April 2016: Caseflow Certification rollout to all VA regional offices
- September 1, 2016: Agile Contract awarded on T4NG with coding exercise
- October 2016: Rolled out eFolder Express to Office of General Counsel and Records Management Center

The Process and Lessons Learned

1. **Understand what people need.** The DSVA team visited the New York Regional Office to collect feedback on Caseflow Certification in October 2015. The team conducted five usability sessions, and used the feedback to improve the tool. The team visited again in December 2015 to gather additional feedback and verify the tool worked as intended in production. Additional usability tests were conducted in the St. Petersburg, Roanoke, Boise and Lincoln regional offices. Testing the service with actual users was critical for building a service that worked for veterans.

2. **Account for training materials and help desk support information.** Prior to rollout, the team needed to prepare training materials for staff who had to use Caseflow. Rather than creating a click-through slide presentation with quizzes, the DSVA decided to record a 5 minute screen share tutorial. Regional Offices provided positive feedback on this format, which they felt was short and specific. In addition to end-user training, the team had to prepare knowledgebase documents for the helpdesk staff who would field support requests from end users.

3. **Launch incrementally.** DSVA established a rollout schedule phased over a month. The team started off with the launch at the New York Regional Office whose employees were most familiar with the tool from the in-person usability

18-F-1517//1322

sessions. From there, DSVA launched in the other regional offices where it conducted remote usability testing. In each subsequent week the team rolled out the application to a larger and larger group of regional offices until it was deployed in all offices.

4. **Ensure application has appropriate monitoring.** The lack of robust application monitoring made it difficult to identify issues with the system. For example, the identity access management service used by the tool went down several times over the rollout period, preventing access to Caseflow. Better monitoring would have allowed the team to identify issues like this before they impacted end users.

5. **Improve automation.** Automation can help improve many aspects of the appeals process (and many similar case processing systems in government). For example, a VA employee shouldn't need to manually re-type information from one system into another system in order to create a form. But there are times in a case processing workflow where human judgment is required. Instead of attempting to account for every edge case, case management systems should automate the most common use-cases, eliminate redundant tasks, and empower staff to use their knowledge and expertise to navigate and resolve tricky edge cases when necessary.

18-F-1517//1323

Simplifying Veteran-facing Services with Vets.gov

The Challenge

Presently, Department of Veterans Affairs' (VA) digital services, such as obtaining a prescription refill, applying for healthcare benefits, checking the status of a claim, and accessing VA forms, are spread across hundreds of public-facing VA websites. Veterans must navigate disparate online systems, remember multiple user names and passwords, and contend with long pages of legalese to access benefits they have earned.

Many of the systems that power these services are outdated and provide a poor user experience. For example, the current digital 10-10EZ form to apply for healthcare was built as a fillable PDF, which requires Adobe Acrobat. The only browser that defaults to Acrobat for PDFs is Internet Explorer, so based on current browser usage, 70% of visitors saw an error message when they tried to apply. As a result, since 2012 only about 8% of all VA healthcare applications were submitted online.

Project Impact Summary

- Many of the systems that power VA's digital services are outdated, and are spread across hundreds of public-facing VA websites.
- In November 2015, the Digital Service at VA launched Vets.gov, a mobile first, cloud-based platform that provides a new way for Veterans to discover, apply for, track, and manage their benefits.
- The initial Vets.gov website included plain language content for education and disability content and several tools: GI Bill Comparison Tool, Facility Location, and a Veteran feedback forum.
- Since then, the vets.gov team has launched 39 products, and reduced release cycle times from 90 days to 7 days.
- In June 2016, a new digital healthcare application was added to Vets.gov. In the first 60 days, 41,000 online submissions were received; an increase from a daily online submission average of 62 per day to more than 500 per day.
- VA is tracking to increase online health care applications from 10% (of 582,000 health care applications received by VA) in 2015 to 50% in 2017.
- In November 2016, the VA Digital Service team will launch several new features including: online application for education benefits, ability to check your disability claim status, prescription refills, secure messaging your health provider, and more.

18-F-1517//1324

The Solution

In November 2015, the VA launched Vets.gov, a new way for Veterans to discover, apply for, track, and manage their benefits. Instead of visiting numerous websites with multiple logins to have their benefits explained to them, Veterans told the USDS design team that they wanted to go to one site to get things done.

The Vets.gov homepage

Specific pieces of functionality planned include the most demanded health and benefits services, such as an accessible health care application that does not require specific software to complete. New functionality will also include claims and appeals statuses, as well as prescription refill services.

18-F-1517//1325

Design and development of vets.gov is led by the U.S. Digital Service at the VA (DSVA) – the first established U.S. Digital Service agency team. It is built with modern, open source tools and is hosted in the commercial cloud. The DSVA is using an iterative development process in which features are continually designed, tested, and integrated into vets.gov. Vets.gov is being built in the open, where Veterans can provide feedback and report bugs directly to the DSVA team, who quickly respond to comments.

Success Criteria	Status
Vets.gov website is available to the public.	Complete. Alpha version launched November 2015. Authority to Operate complete.
Launch digital healthcare application.	Complete. Vets.gov digital healthcare application launched June 2016.
100% of relevant content and front-end functions migrated from 514 existing public-facing VA websites.	In progress. Content related to disability benefits, education benefits, and careers and employment has been migrated to date.
Measurably improved Veteran experience.	In progress. The new online health care application has increased online submissions from 62 per day to more than 500 per day. Metrics collected will include bounce rates, page views, percentage of applications submitted online, volume of support requests to VA call centers.

Milestones

The initial vets.gov website was launched on November 11, 2015. It is a cloud-based platform with a modern technology stack. Immediate benefits and features included the following:

- Mobile-responsive website
- 508 compliance improvements

18-F-1517//1326

- GI Bill Comparison Tool
- Facility Locator
- Disability Benefit content rewritten in plain language
- Education Benefit content rewritten in plain language
- Feedback forum to collect Veteran feedback on the website

Since November, the team has been conducting ongoing research with Veterans and delivered additional content and features on the site, including employment services, the crisis hotline, and most recently the healthcare application.

On June 30, 2016, a new digital healthcare application was added to Vets.gov to enable Veterans to apply for healthcare online, solving the problems that prevented many Veterans from using the previous online application. As a result, the number of Veterans applying for health care online increased from 62 per day to over 500 per day. VA is now on track to increase the percentage of Veterans applying online from 10% in 2015 to over 50% in 2017.

Migration will continue throughout 2016, focusing on the highest demand Veteran services including functionality such as applying for healthcare and obtaining prescription refills.

The Process and Lessons Learned

1. **Understand what people need.** Vets.gov is being designed based on Veteran feedback. The vets.gov team works with Veterans regularly on research activities including usability testing, card sorting, and contextual interviews, using a combination of remote / in-person sessions and individual / group sessions.

2. **Build the service using agile and iterative practices.** Vets.gov is being iteratively developed, with new functionality released incrementally and refined based on feedback from Veterans. To manage this iterative process, the vets.gov team uses industry-standard techniques such as sprint planning and stand-up meetings for each vets.gov product team. These processes enable open communication and fast problem resolution. The whole team holds retrospectives every quarter to review progress and troubleshoot challenges.

3. **Engage stakeholders across the agency.** As a change management tool, the team opened bi-weekly vets.gov 101 briefing to all VA employees and stakeholders. To ensure leadership was fully engaged, the team had regular meetings with the Secretary and Deputy Secretary. The team was fully transparent in its planning and reporting by opening up the vets.gov roadmap to anyone at

18-F-1517//1327

the VA and offering status reports daily to anyone at the VA. Finally, weekly VA Change Management working sessions with communications leads and VA stakeholder meetings helped the team bring diverse players to a common understanding of the vision and goal to ensure success.

18-F-1517//1328

Providing Secure Access to IRS Taxpayer Information

The Challenge

Over 150 million taxpayers interact with the IRS each year. The IRS wants to offer taxpayers digital services such as online access to individual tax records and tax refund statuses. There is clear demand for these services from taxpayers – for example, the "Where's My Refund" online tool is one of the most popular Federal Government websites, with over 200 million requests in 2015. However, providing online taxpayer services is difficult due to the challenge of distinguishing a legitimate taxpayer from an identity thief who may try to steal information held by the IRS to commit fraud. IRS currently withstands more than one million attempts to maliciously access its systems each day.

One important IRS digital service is Get Transcript Online. The tool lets taxpayers access their official tax history, which can be needed for student loan applications, mortgage paperwork, or even filing the current year's returns. In May 2015, widespread unauthorized access of the tool forced IRS to take it offline. After analysis, IRS determined that bad actors had been using taxpayers' personal information stolen from data breaches outside the IRS to circumvent the tool's identity verification process. As a result, some taxpayer information was released to unauthorized users, who used the data to commit tax return fraud.

Creating a new authentication system that solves the difficult challenge of verifying the identity of individuals seeking to use IRS services was a top priority for the agency. Not only would this allow the IRS to restore access to the Get Transcript Online tool, but a method for securely identifying taxpayers is a prerequisite for many future digital services that the IRS is seeking to build for the American people.

One approach considered early in the Secure Access project was to add a "PIN in the mail" step to the user registration process, in which the IRS would mail an activation code to a taxpayer's physical address. The IRS was not satisfied with this solution because it wouldn't provide a better user experience than the default process of simply mailing tax transcripts directly to taxpayers that request them, a process which takes 5-10 days. The IRS wanted a solution that would allow taxpayers to get access to their own data in minutes, not days.

18-F-1517//1329

Project Impact Summary

- In May of 2015, the IRS removed the ability for millions of taxpayers to get online access their tax transcript because the "Get Transcript Online" service had been abused by unauthorized users.
- One option considered to secure the service would be to physically mail transcripts or account PIN numbers. However the IRS wanted a solution that could be completed in minutes, not days.
- A team of three USDS personnel worked with IRS beginning in October 2015 to help design and implement a new Secure Access online process.
- With the help of the USDS team, IRS executed a controlled launch in which the new service was tested with small groups of real users prior to full launch. The team also implemented fine-grained error-tracking and log monitoring. With this approach, USDS helped IRS achieve a 4x reduction in the error rate prior to full launch.
- The new Secure Access process takes an average of 12 minutes for users to complete, compared to the 5-10 calendar day wait for mailed transcripts without Secure Access.
- "Get Transcript Online" was returned to service for all taxpayers using the new Secure Access process in June 2016.
- As of August 22, 2016, taxpayers have accessed over 2.7 million transcripts using the online Secure Access process.
- IRS plans to re-use the Secure Access process for four additional services in IRS' e-Services suite.

The Solution

Recognizing the importance of secure online access, the IRS asked to partner with experts from the USDS in determining how to strengthen their authentication protocols while remaining convenient for taxpayers. Together USDS and IRS outlined the characteristics of a tool called "Secure Access": a user verification process using strong identity proofing and two-factor authentication in line with both industry best practices and federal standards from OMB and NIST.

The new system adheres to the "Level 3" standards of Electronic Authentication Level of Assurance, as defined by NIST in SP 800-63-2. This level of assurance requires an individual to demonstrate control over a physical object (i.e. "something you have") in addition to demonstrating knowledge of personal information such as name, birth date and social security number (i.e. "something you know"). The old system adhered to

18-F-1517//1330

LOA2, which allowed access to the system using personal information as well as knowledge-based multiple choice questions. This level of assurance proved insufficient, because some of the personal information used to verify users' identities in this approach had already been compromised in various data breaches from sources other than the IRS.

Using Secure Access to protect sensitive applications like Get Transcript Online would enable taxpayers to have convenient, real-time access to their transcripts without making that information vulnerable to automated fraudulent attacks. Working side by side with the agency, USDS helped IRS deliver the Secure Access project following principles from the Digital Services Playbook. These proven approaches enabled the IRS to efficiently deliver the Secure Access project in a timely manner. In June of 2016, the IRS launched Secure Access and brought Get Transcript Online back into service.

Success Criteria	Status
Restore online access to tax records in a manner that is secure against automated attacks (implementation of the NIST Level of Assurance Level 3 standard)	Complete. Service launched in June 2016. As of August 22, 2016 taxpayers have accessed over 2.7 million transcripts.
Build an account creation process that takes less than 15 minutes for a user to complete.	Complete. Account creation takes an average of 12 minutes, vs. 5-10 days for mailed transcripts or PIN numbers.
Implement error tracking and log monitoring. Collect and report daily business metrics.	Complete. Daily statistics on attempts, pass rates, error rates and overall traffic are collected and disseminated. Error tracking and log monitoring implemented. Phased launch strategy resulted in fourfold reduction in error rate.
Secure Access process used for at least one additional IRS service in addition to Get Transcript Online.	Complete. Secure Access is now used for the "Get an Identity Protection PIN" service in addition to Get Transcript Online. IRS also plans to implement Secure Access for four additional services in IRS' e-Services suite (Registration Services, e-File Application, Transcript Delivery, and TIN Matching).

18-F-1517//1331

Milestones

- October 2015: Discovery Sprint completed
- November 2015: Project start date
- February 2016: Secure Access protocol code completed
- March 2016: Internal employee test
- May 2016: Service launched to production, beginning controlled phase-in approach
- June 2016: Service launched to all users

The Process and Lessons Learned

1. **Assign one leader.** The IRS recognized the need for a single executive to help provide consistent oversight over all authentication and authorization needs across the many IRS functions and channels. They created the Identity Assurance Office, led by a senior IRS executive with experience working with both business and information technology groups. USDS worked side by side with this executive, helping clarify the business, product, process, and technical decisions that come with the responsibility of meeting user demands. USDS also worked with partners at OMB and NIST to get relevant background information that would help this leader make decisions that would meet federal standards while also meeting both user and business needs.

2. **Understand what people need and design a simple and intuitive service.** USDS worked with the IRS team to maintain constant focus on taxpayer needs. At the beginning of the project, USDS gathered input from the United Kingdom's Government Digital Service to inform early directions and learn from this organization's hard-won experience. One of the key insights from the U.K. team proved particularly valuable. The U.K. team learned it was important to set user expectations about how the authentication process would work up front, and to provide graceful alternatives if the user cannot or does not wish to continue with the online authentication process.

   USDS worked with the IRS to create draft user flows and tested them with users on a weekly basis. USDS improved the navigation, flow and messaging based on these tests. For example, an early prototype confused taxpayers by stating that authentication would require a "Credit card or auto loan, mortgage, home equity loan account number." In usability tests, the team learned that taxpayers thought they needed the account number for the credit card, not just the last eight digits of the credit card itself. The team changed the wording to be clearer. The IRS will

18-F-1517//1332

continue to use this iterative design process to help determine which features and fixes should be prioritized.

3. **Build the service using agile and iterative practices.** In addition to the iterative design process described above, at the suggestion of the USDS, the IRS used a phased launch process to test and refine the Secure Access protocol before its full launch. Initially, the agency limited access to the authentication system to only IRS employees. This controlled test allowed the team to get end-to-end user data that accelerated debugging and improvements.

4. **The USDS worked together with developers and business analysts to understand how users were getting stuck in order to improve the process.** An example of an issue that was discovered and fixed in this controlled launch was in a data entry field. When users were prompted to enter their account number, some users included the "#" character when typing the number. This would generate an error message that explained the "input was too long," confusing users. This problem did not surface in internal quality assurance testing, and would not have been discovered without letting real users interact with the system prior to full launch. The team fixed the problem and redeployed the improved code to another cohort of internal users. After this internal test, the IRS used a public beta period where the improved Get Transcript Online service was offered to a small percentage of public visitors to the IRS website. This beta period allowed the team to fix even more issues. This iterative process was used to identify and fix many subtle errors and points of confusion prior to full launch.

5. **Use data to drive decisions.** Collecting good data on how users were interacting with the system was a key to success. With USDS assistance, the IRS developers implemented fine-grained error codes and log monitoring. With this data, the team could categorize bugs and list the most common errors, allowing the team to prioritize its efforts. In one such case, a bug that resulted in a small number of users in the public beta test being unable to register was identified and eliminated. In this case, USDS engineers examined the code and speculated that an input validation filter on one of the field items had been accidentally set too strictly, rejecting some valid inputs. An IRS developer used the error monitoring data to identify that the error was highly correlated with specific versions of the Firefox web browser. With these insights, the team was able to identify the root cause of the error and deploy a fix before the tool's public announcement, saving hundreds of users a day from having the same issue.

   Between the initial deployment of the Secure Access protocol and the full public launch, iterative development coupled with good monitoring allowed the IRS to

18-F-1517//1333

achieve a fourfold drop in the error rate. The agency will continue to monitor errors and prioritize effort based on this data.

18-F-1517//1334

Improving the Visa Processing System at Department of State

The Challenge

The Department of State (State) protects the lives and interests of U.S. citizens overseas and strengthens the security of U.S. borders through the vigilant adjudication of visa and passport applications. State provides a range of services to U.S. citizens and foreign nationals, including issuance of U.S. passports and Consular Reports of Birth and Death Abroad and adjudication of nonimmigrant and immigrant visa applications. These processes largely are conducted through a collection of custom applications that depend on a system called the Consular Consolidated Database (CCD).

Many government systems, including the CCD, were designed at a time before most modern technologies to support distributed data processing were available. As a result, CCD's technical approach – innovative at the time it was implemented – deviates from what are now industry best practices. Over time, development focused on adding new features rather than modifying the underlying platforms and tools.

The integration of various components made the CCD progressively more complex. As a result, it became more difficult to ensure new features were integrated in a high-quality, easily maintainable manner. As demand increased, some tools were not able to be improved upon in a timely fashion.

Project Impact Summary

- In June 2016, the USDS team began discovery work around how to improve the visa application process. The team honed in on better ways to update applicants and petitioners on case status by making adjustments to a tool built in 2012.
- Over the past year, the CEAC Visa Status Check site received over 3 million visits per month from users ranging from petitioners in the United States to applicants across the world.
- The National Visa Center, a visa application processing center run by the Department of State, receives approximately 9,000 phone calls a day. The vast majority of those calls are about a visa applicant's case status.
- The USDS team, in partnership with the Bureau of Consular Affairs, is in the process of engineering improvements to the tool that will show users better

18-F-1517//1335

information about their case status and how to advance to the next stage of the application process.

- The USDS team performed robust user testing of the new status tool and tested how improved information using plain language may help cases move more quickly through the appropriate parts of the process.
- The status tool will launch soon. We will measure the impact of the tool against several metrics, including how it impacts the National Visa Center's call volume.

The Solution

USDS worked closely with State's Bureau of Consular Affairs' Office of Consular Systems and Technology (CST), which supports, develops, and maintains the technology that enables a global network of consular systems to support U.S. consulates and embassies, domestic visa processing centers, and domestic passport processing agencies and centers. CST already had a number of viable plans to improve overarching stability of the CCD and related applications, but attempts to execute these plans had been stymied by the system's complexity. USDS served as technical consultants, both vetting possible solutions and advising on industry best practices and as an empowering authority facilitating communication across divisions and organizations.

Success Criteria	Status
Standardize software development processes and tooling, enabling the Federal Government to have better visibility into contractor-developed custom software.	Completed. Established central source control repositories on a unified source control system. Completed a pilot that has improved developer workflows and allowed greater oversight into how code is being developed.
Transition how information is batched and sent to partner agencies to ensure there are no artificially created backlogs.	Completed. Changes made from both ends have been implemented and information is more efficiently transferred between agencies.
Immigration process and status is clear and comprehensible to applicants.	Ongoing. USDS team is currently implementing improvements to an existing tool that should more clearly communicate case status to applicants.

18-F-1517//1336

Milestones

- December 2015: USDS began engagement to improve information security of various State applications.
- February 2016: USDS began exploration of what kind of developer tools were needed within State to improve engineering practices.
- March 2016: State received USDS recommendations for improved developer tools, including usage of version control software.
- April 2016: USDS began assisting a State vendor with implementation of a version control software pilot.
- April 2016: USDS began discovery work on how to improve how State transmits information for Security Advisory Opinions with partner agencies.
- June 2016: USDS began determining ways to improve how visa status information is shared with applicants, petitioners, and their agents.
- June 2016: Technical implementation of the Security Advisory Opinion data sharing process began.
- July 2016: Technical implementation of improvements to visa status check tool began.
- September 2016: Completion of the technical and business process changes for the Security Advisory Opinion data sharing process.
- September 2016: USDS completed work on a pilot that saw a number of contractors using modern software development tools in the form of version control software.

The Process and Lessons Learned

1. **Working with and Empowering the Agency:** State identified a number of areas where it could improve its information security. USDS provided assistance in the form of consultation on system remediation and coordination of implementation. USDS also worked closely with teams within State to identify how to prioritize various kinds of remediation that needed to be implemented and how to rank ongoing concerns. Using these techniques, State has markedly improved its defensive posture.

2. **Breaking Agency Silos to Solve Problems Together:** In many cases both the technical expertise and the most appropriate solution were already present within the organization. However, in an agency the size of State it is sometimes difficult to convene these groups and share solutions to senior leadership and across the agency. USDS conducted extensive site visits to bring various branches and contractor groups across State together, and with State leadership's help was able to create cross-team collaboration that sped up the development and deployment of solutions. The project to modernize developers' tools, for

18-F-1517//1337

example, is a collaboration between multiple divisions within CA/CST: Configuration Control, Systems Engineering and Integration, and Service, Systems and Operations.

3. **Technical Vetting and Evaluation:** USDS provided State program and project managers with objective technical advice. This gave State better accountability and communication among contractors. Since problems were often spread over applications and systems governed by several contracts, government managers heard different technical explanations. USDS engaged in several "fact finding missions," allowing State to use this information to prioritize tasks effectively.

4. **Embrace pilots:** Pilots are great opportunities to perform experiments in a contained, structured way. The ability to experiment is essential when bringing on new tools, services, or methodologies. It's not clear which will work best in a given environment, so experimentation is essential to bringing new tools, services, and methodologies to an organization. Knowing that the results will be used to determine if a pilot will continue helps stakeholders embrace new methods of doing things.

5. **Test early and often:** Manual and automated testing are essential parts of the software development process. Increasing your test coverage makes it easier to deploy a tool or functionality quickly and securely. We are hopeful that by working with stakeholders and contractor teams, we can improve the testing culture for how Department software is developed.

18-F-1517//1338

Helping CMS Implement Congressionally Mandated Medicare Payment Changes

The Challenge

In April 2015, Congress passed the Medicare Access & CHIP Reauthorization Act of 2015 (MACRA), changing the way Medicare pays doctors for services rendered to patients enrolled in the Medicare program. The act implements changes designed to reward health care providers for giving better care, not just more care. These changes will impact a large percentage of Medicare Part B payments, and the Centers for Medicare & Medicaid Services (CMS) seeks to ensure the transition from the current payment program to the new system is simple, clear, and effective.

Project Impact Summary

- Implementation of the Medicare Access and Chip Reauthorization Act of 2015 required a transition of payment programs that would impact a large percentage of Medicare payments to doctors.
- CMS engaged the USDS team to draw on best practices from other large program implementations.
- CMS created an integrated project team that combines policy and operations, and uses agile methodologies and other modern technology practices.
- The development team has employed user research, user need analysis and constant iterative feedback loops with users to ensure transition success.
- On October 14, USDS helped CMS released the Final Rule for implementing MACRA concurrently with a plain language website describing the rule. The website serves two purposes: first, to help clinicians and their partners easily understand how MACRA impacts them and, second, to serve as a single entry point for clinician interaction with the program in the future.
- The MACRA implementation is still on-going and iterative development will continue throughout 2017.

The Solution

MACRA implementation is an important priority at CMS. USDS is helping CMS take an implementation approach that draws best practices learned from implementing other large programs, including HealthCare.gov and the adoption of the 10th revision of the

18-F-1517//1339

International Statistical Classification of Diseases and Related Health Problems (ICD-10) standard. Key priorities include widespread user research and user needs analysis, an integrated project team across CMS responsible for program delivery from policy to operations, a tight iterative feedback loop with users to inform program design and ensure that it is clear and accessible, and incorporation of modern technology best practices.

Success Criteria	Status
Contracts for key elements of MACRA implementation are agile and responsive to evolving program needs.	In progress. CMS has successfully used agile acquisition practices across most of the contracts for the MACRA program.
Project team is integrated and running off of a shared roadmap for execution, including user research, policy, procurement, operations, technology, and analytics.	In progress. CMS has identified a product owner for MACRA implementation. CMS staff and contractors work on an integrated team.
Modern technology development best practices are being used in the creation of program infrastructure.	In progress. USDS assisting CMS staff and contractors to implement best practices in design and engineering.

Milestones

- February 2016: USDS Discovery Sprint/Project Started
- May 2016: Development work started
- October 2016: Final Rule with Comment and website concurrently launched

The Process and Lessons Learned

1. **Go where the work is.** The USDS team has pushed for extensive collaboration and information sharing between the USDS, CMS, and its contractor teams. The USDS team works alongside CMS staff and contractors on an integrated team at least four days a week in a shared space to facilitate this goal.

18-F-1517//1340

2. **Engage agency leaders and policymakers in the process.** The USDS team works hand-in-hand with CMS leadership on the program. The team is helping to ensure that implementation details, technical trade-offs, and operational complexity are communicated effectively to the whole team, including those writing policy.

3. **Identify a product owner.** CMS identified a single product owner for the implementation of the law, which has facilitated faster decision making.

4. **Provide contracting officers with agile acquisition training.** The CMS team was aware of agile acquisition practices, and their ability to implement agile contracts was significantly helped because one CMS contracting officer had already gone through the USDS agile acquisition training program. CMS has successfully utilized agile acquisition practices across most of the contracts for the MACRA program. The head of the division has further requested more training in agile contracting for the entire team.

18-F-1517//1341

Reducing Inefficiency in the Refugee Admission Process

The Challenge

In Fiscal Year 2016, President Obama set a ceiling of admitting 85,000 refugees into the United States. This represented a 15,000 person increase over the previous fiscal year's ceiling, and this increase depended upon improving the efficiency of the refugee admissions process.

One of the most impactful improvements was the introduction of the digital approval process for refugee applications. Previously, Department of Homeland Security (DHS) officers were only able to approve refugee registration forms using an ink approval stamp in the field where the refugee file is physically located. 57% of cases are finalized on a different day than the DHS field interview. In many of these cases the requirement for an ink approval stamp added an unnecessary delay of up to eight weeks after all security checks had been completed, as cases waited for a DHS officer to travel back to the field location where the file was located to stamp it approved.

Project Impact Summary

- In December 2015, USDS, the State Department, and the Department of Homeland Security established an interagency Refugee Coordination Center (RCC) staffed with representatives from each agency.
- The RCC began working on a prototype for digital approval of cases in January 2016 and launched the product for DHS use in June 2016.
- By September 30, 2016, 11,571 individuals had been digitally-approved, helping the Administration meet its refugee admissions goals while maintaining integrity in the process. Furthermore, the digital approval process codified rigorous security standards, granted DHS flexibility of when and where it can spend time doing administrative work, and saved the Department of State's Resettlement Support Centers time and money by eliminating the need to prepare and ship case files for ink approval stamping.
- State Department Resettlement Support Centers (RSCs) processing these cases stated that the following amounts of time were reduced in the admissions process as a result of the launch of the digital approval process: Bangkok: 1-2 months; Malaysia: 1-2 months; Middle East and North Africa: 1-6 weeks; South Asia: 15 days; Latin America: 15 days; Africa: 12 days.

18-F-1517//1342

The Solution

The digital approval process enables DHS officers to digitally-approve a refugee registration form without having to physically travel to apply an ink stamp on paper. The solution was created by granting DHS editing rights to the State Department's refugee case management system for the first time. Filters ensure that only cases ready to be approved appear for DHS to digitally approve.

In order to convert the manual process into a digital process, the RCC worked with DHS officers to convert all of the manual steps to approve a case into the new digital approval feature. These included:

Checking security statuses

In the manual process, DHS officers are required to physically review a security report for each individual on a case and annotate the page attesting that they have reviewed each page. In this digital approval process, DHS officers electronically affirm they have reviewed all security statuses and the case file, which then enables them to click the digital approval button.

Updating the hard copy form

In the manual process, DHS officers have a paper form that is a history of all actions made on a case. In the digital process, once a digital stamp is applied, the system automatically generates a new digital file for the case, including the time and date the case was digitally-approved, and is included in the case's physical file by the State Department.

Approving the I-590

In the manual process, DHS officers physically approve a refugee registration form (Form I-590) by applying an ink stamp to the approval block on the form. In the digital process, DHS officers click "stamped approved" and the system securely and automatically-generates an individual-level approval page with the time stamp and name of the approving DHS officer. The RSC staples this file to the front of the refugee form, which Customs and Border Protection reviews upon the refugee's arrival at a port of entry in the United States.

Approval Letter

In the manual process, once a case is ready for approval DHS officers initial an approval letter. State Department Resettlement Support Centers then date the letter before

18-F-1517//1343

scanning it and then delivering to the refugee. In the digital process, the system automatically-generates an approval letter with the approving officer's initials and the time stamp when the case was approved, and it is automatically-saved in the case's digital file. The Resettlement Support Centers print and deliver the approval letters to the refugee.

The Role of the RCC

In addition to these process modernizations, USDS assisted with data modeling to predict the number of people who would benefit from digital approvals in order to justify dedicating engineers' time to develop this feature. USDS also designed the system requirements, created prototypes, and coordinated agency-wide approvals for the project. USDS then worked with State Department engineers to develop the new features, and with DHS officers to test the features prior to launch. USDS assisted with the phased roll-out of the digital feature, including training of DHS officers and development of Standard Operating Procedures (SOPs). Finally, USDS ensured that USCIS notified all stakeholders within DHS to prepare components for these changes prior to the first digitally-approved cases arriving in the United States.

Success Criteria	Status
Reduce the time between the date a case is ready for approval and the date it is approved to under two weeks.	On track. In August 2016, of all cases that were digitally-approved, 74% were approved in five days or less and 56% in two days or less. Of the 124 cases that took more than 15 days to digitally approve, 77% did not need to travel until January 2017 or later.
Reach 8,000 individuals approved digitally before the end of the fiscal year.	Complete. 11,571 individuals were digitally-approved by the end of the fiscal year.
Ensure at least 20 officers were part of the digital approval pilot.	Complete. By the end of the pilot, more than 60 officers were trained and had permission to use the digital approval process.

Milestones

- January 2016: Began prototyping and requirements gathering for the digital stamp

18-F-1517//1344

- March 2016: Finalized all data analysis, cost benefit analysis, completed requirements
- May and June 2016: State Department engineering team developed digital approval feature
- June 2016: Conducted user testing and fixed bugs in the system
- June 2016: Digital approval process launched
- September 30: Digital approval process pilot ends and full roll-out began

The Process and Lessons Learned

1. **Engage stakeholders across the agency and collaborate with subject matter experts.** Engaging stakeholders across the agency and working with civil servants who are subject matter experts was essential for the success of this project. In this case, the concept of digitally processing cases had previously been identified by individuals at DHS as an opportunity to increase efficiency. Identifying and collaborating with these individuals allowed USDS to make progress faster.

2. **Keep the scope narrow for the minimally viable product (MVP).** Despite pressure to expand the scope of the MVP that was prototyped, development remained focused on the most critical features for refugee officers and refugees. Throughout the development process, USDS focused on core user needs, replicating the existing physical process into a digital experience. This narrow focus ensured that work flows would remain largely unchanged for refugee officers.

3. **Understand users' needs by testing with actual users.** The digital approval process was built with input from internal users to ensure their feedback was understood and addressed prior to launch. While quality assurance testing by Department of State engineers was critical, USDS' time spent with DHS end users was important for uncovering a variety of issues that would not have been found through engineering team testing alone.

4. **Rely on pilots and build up to a successful launch.** USDS relied on an initial pilot period (from June 24th through September 30th) with limited users (at first only one user and by the end more than 60) to identify any new glitches. Additionally, USDS worked with DHS to develop Standard Operating Procedures and video, teleconference, and in-person trainings to ensure ease of use and clear understanding of the new digital process. Once the digital approval process was judged to be successful and stable with the small pilot group, it was rolled

18-F-1517//1345

out more broadly to additional users. There was unanimous support to roll out the digital approval process to all trained and eligible users in Fiscal Year 2017.

18-F-1517//1346

Helping Students Make More Informed College Choices at Department of Education

The Challenge

For students, higher education may be the single most important investment they can make in their futures to ensure they have the knowledge and skills needed to compete in an increasingly global marketplace. College is the surest path to becoming part of America's middle class and for this reason, selecting a college is an incredibly important decision for many people. But, many potential college students and their families do not have the advisors or resources to help them find a college that will serve them well.

With college costs and student debt on the rise, the choices that American families make when searching for and selecting a college have never been more important. Yet, students and the organizations that serve them struggle to find clear, reliable, and comparable data on critical questions of college affordability and value, such as whether they are likely to graduate, find middle-class jobs, and repay their loans. At a time when America needs colleges to focus on ensuring affordability and supporting all students who enroll, many of the existing college rankings instead reward schools for spending more money and rejecting more students. Additionally, college leaders and state policymakers who seek to improve institutions' performance often lack reliable ways to determine how well their schools are serving students.

To address this challenge, the Department of Education sought to redesign the College Scorecard.

Project Impact Summary

- The USDS team at the Department of Education, with help from 18F, launched the College Scorecard to help students and their families make more informed choices about where to go to school.
- The Scorecard makes comprehensive data on college costs, graduation rates, graduate debt, repayment rates, and post-college earnings accessible to help students choose a school based on access, affordability and outcomes.
- The project drew on hundreds of interviews with students, parents and guidance counselors to ensure that the product would fit their needs.

18-F-1517//1347

- In its first two weeks, College Scorecard attracted over 850,000 unique users, a major uptick from the 160,000 who used the prior version of the tool the entire year before.
- The project opened the data to the public and made an API available specifically for third-party developers to build more applications to help students and policymakers. More than a dozen organizations have built new tools using this data.
- Google has now integrated College Scorecard data so that it shows up front and center in the results of hundreds of millions of education-related searches.

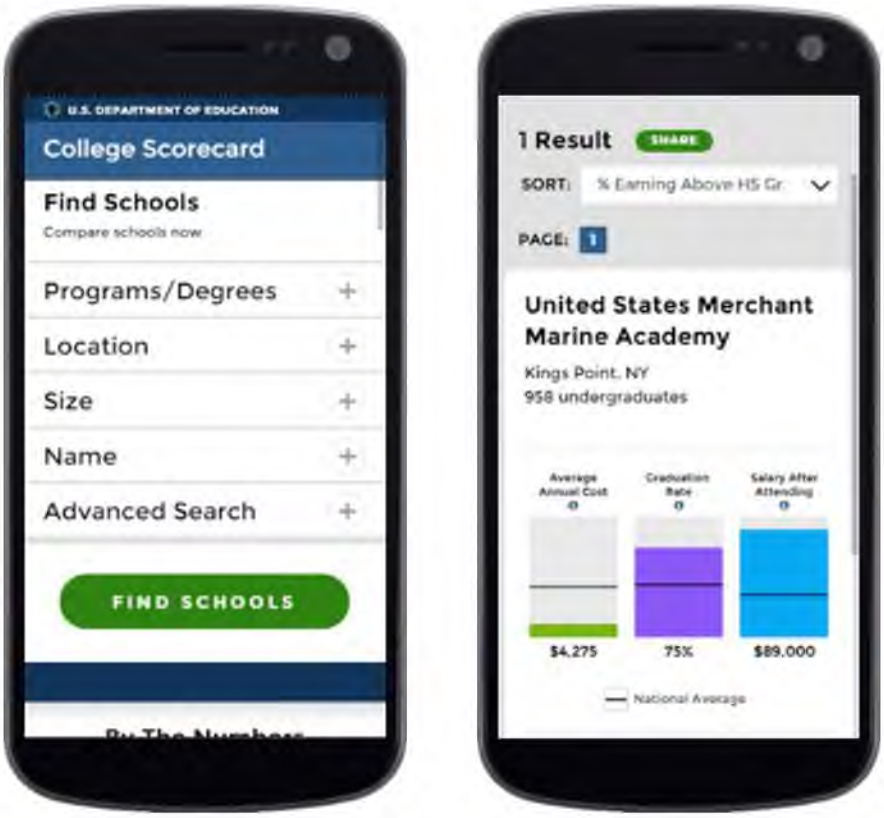
The Solution

The new College Scorecard was redesigned with direct input from students, families, and their advisers to provide the clearest, most accessible, and most reliable national data on college costs, graduation rates, and post-college earnings. This new College Scorecard can empower Americans to rate colleges based on what matters most to them; enable policymakers and the public to highlight colleges that are serving students of all backgrounds well; and focus greater attention on making a quality, affordable education within reach. The new tool for assessing college choices, with the help of technology and open data, makes it possible for anyone—a student, a school, a policymaker, or a researcher—to evaluate an institution on the factors that matter most to them.

The public can now access the most reliable and comprehensive data on students' outcomes at specific colleges, including former students' earnings, graduates' student debt, and borrowers' repayment rates. This data is published through an open application programming interface (API), enabling researchers, policymakers, and developers to customize their own analyses of college performance more quickly and easily.

More than a dozen organizations are using this data to build new tools. For example, Scholar Match, Propublica, and College Abacus—three college search resources—are using the new, unique data to help students search for, compare, and develop a list of colleges based on the outcomes data that the Department of Education made available for the first time through an API. InsideTrack, comprised of a team of coaches and consultants working to improve student outcomes by helping students find the institutions that are right for them, uses the data to develop and implement effective student-centered initiatives.

18-F-1517//1348



The College Scorecard

The Department of Education plans to continue releasing new College Scorecard data and promoting use of these new access, affordability and outcome metrics.

Success Criteria

Success Criteria	Status
Engage a diverse set of students and their supporters, especially high-need, low-income and first-generation college-goers.	Ongoing. In the first two weeks the Scorecard was launched, it was accessed by 850,000 users. The previous version of the tool received 160,000 total users in the previous year.
Educate the marketplace and shift focus to key outcome metrics and institutional performance	Ongoing. External organizations and third party developers are making use of this new data in their tools and research.

18-F-1517//1349

Success Criteria	Status
Enable more informed college matching	Ongoing. As of September 2016, 1.5 million unique users have accessed the tool. The previous version of the tool received 160,000 unique views a year.
Foster continuous improvement	Ongoing. New data was released to the Scorecard in September 2016. All Scorecard information is now appears in search results for colleges.

Milestones

- April 2015: Project Start Date.
- July 2015: Code Start Date.
- September 2015: Go-Live Date.
- May 2016: USDS Project End Date.
- September 2016: New data released to Scorecard. All data indexed and searchable.

The Process and Lessons Learned

- **Understand what people need.** USDS, Ed, and 18F built College Scorecard by working with users at every stage of the project to find out how they made decisions about college. The team met with students (both high school and adult), parents, guidance counselors and advisors, open data users, and people who wrote to the President about their college search experiences. Long before the first line of software code was written, the team was working with students, testing paper prototypes to make sure they were as easy-to-use as possible.

18-F-1517//1350

Getting feedback on a paper prototype of the new College Scorecard.

- **Build services using agile and iterative processes.** The Department of Education built the College Scorecard using agile development methodology. To deliver the right product — what students actually need — as efficiently as possible, the team built the new College Scorecard using an approach that allowed the team to work in short iterations, and to test, scale, and design the tool with a process that could adapt to changes in technology and user needs. The team maintained a project rhythm of two week iterations, with daily stand up meetings to coordinate progress.

- **Run a developer beta.** USDS ran a beta specifically for developers — giving them a chance to test the data and documentation and flag opportunities to make it even easier to use. The feedback from the developers made it possible to release the data in a way that led to easy re-use by third parties.

- **Launch a minimum viable product (MVP).** The team focused on launching a MVP, building the right products to meet customer needs as efficiently as possible. This approach allowed the project to launch with less than 3 months of development time. The team built the project mobile-first and focused on the most critical feature set and information that each user type advocated for.

- **Release open data, and build services using the same APIs offered to the public.** Rather than focusing solely on creating a user-facing website, the team

18-F-1517//1351

also created documentation for, and released, open data for over 7,300 colleges and universities, going back 18 years. This made it possible for third-parties to incorporate the data into their own products and tools, increasing the chance that the information makes it to users wherever and whenever they might be looking for it.

To make it easier for third parties to integrate this data, Department of Education published an API. This API serves both as the engine for the College Scorecard itself as well as a source for external software developers or researchers who want to use the data in their own digital products. The College Scorecard effort is one of the first government digital services that not only releases open data, but also builds a user-facing tool on top of the very same API it provides to the public. This is a common practice used by American's best technology companies.

18-F-1517//1352

Modernizing the Department of Defense Travel System

The Challenge

The Defense Travel System (DTS) provides travel for all Department of Defense (DoD) employees (excluding permanent changes of station). While the DTS does provide end-to-end travel and expense functionality, the antiquated system provides a poor user experience and limited reporting capability. The system has long been a pain point for DoD travelers and officials, and has been scrutinized by lawmakers and auditors. For example, after the Government Accountability Office determined that DoD had overestimated savings for DTS and failed to fix implementation problems with the system nearly a decade ago, DTS added fees for the user and prevented travelers from quickly making changes to their reservations. Lawmakers have required the DoD to improve Defense travel through the creation of the Defense Travel Management Office (DTMO) and providing them with the Defense Travel Pilot Authority to find ways to improve the system and agreements that govern Defense travel.

Currently, the Department of Defense's travel spend is over $8.7 billion per year. Of this spend, $3.5 billion is handled through the DTS, with a per-transaction cost around $10. In addition, there are over 1600 pages of DoD travel regulations. Despite this, about 100,000 unique users access DTS daily, according to the DoD website.

The complexity of the Joint Travel Regulations imposes a challenge for standard DoD users, as well as Authorizing Officials who administer and authorize travel. Many of the policies make it difficult to apply commercial best practices to the system. For example, the policy precludes the integration of industry-standard features like restricted fares, which could ultimately lead to higher cost savings across the department.

Project Impact Summary

- The Department of Defense has long needed to improve the costly and cumbersome system used to book, expense, and manage travel for its employees.
- In March 2015, the Digital Service team at the DoD started working with agency staff to identify a new, commercial tool to better manage travel, and agreed to oversee a pilot test of the new system.
- At the same time, DoD worked to simplify its complex travel policy, with an eye toward saving millions of dollars and delivering a better user experience.

18-F-1517//1353

- In June 2016, the new software-as-a-service travel tool and streamlined policy were in place, and a pilot opened for "basic travelers." Both are still being refined.
- This project demonstrates the potential of pairing policy development with technology implementation to produce more efficient outcomes, and reinforces the principle that using commercial software when minimal customization is required can save the Federal Government significant time and money.

The Solution

To reduce costs and improve the customer experience, DoD is seeking to modernize its travel system with a commercial software-as-a-service (SaaS) product. At the same time, DoD has committed to simplifying the travel policy under the Joint Travel Regulation (JTR). These changes have the potential to save hundreds of millions of dollars per year and improve satisfaction of Defense travel customers. The Deputy Secretary of Defense has directed the relevant human resources and travel offices to complete the policy review and the initial technical transition. The USDS' Defense Digital Service team assisted DoD and its DTS contractor in identifying a commercial vendor that could meet its requirements without requiring expensive customization.

The Defense Digital Service team is also helping DoD pilot this new system. The pilot, now underway, is focused initially on a small population of "basic travelers" using a streamlined travel policy subset. Over time, the project will scale in size and complexity. Concurrently, an effort is underway to considerably simplify the JTR by consolidating the types of travelers.

Success Criteria	Status
New DTS tool released	In progress. Tool has been identified, and is currently being piloted.
Policies governing DoD travel simplified	In progress. An effort is underway to considerably simplify the JTR by consolidating the types of travelers.
Increasing DTS customer satisfaction rating	In progress. As of June 2016, pilot is underway.

18-F-1517//1354

Success Criteria	Status
All travel request processed in new DTS system	Incomplete. Small pilot underway.
Improve data collection to enable better market position with travel vendors	Incomplete. Underway.

Milestones

- March 2015: DTS Sprint begins.
- June 2016: First user booked travel in the new system.

The Process and Lessons Learned

1. **Digital services are only as good as their underlying policy.** Many of the challenges with the current DTS system stem from the complexity of the Joint Travel Regulations. Without updates to this policy, it will be difficult to modernize the DTS. For example, the Joint Travel Regulations require pre-obligation, which is the act of obligating funds for travel prior to the trip based on the trip's estimated cost. This pre-obligation estimate is intended to prevent a trip from costing more money than is available, and includes transportation, hotel, per diem, and incidentals. However, many standard commercial travel solutions cannot easily accommodate pre-obligation estimates, so the DoD is working to change the current policy requirements to avoid requiring system customization. One solution being proposed is to estimate total travel costs and make a budgetary hold on the funds so that approving official will not approve trips in excess of an approved budget. Another potential solution also includes making an estimated bulk obligation based on historical expenditures.

2. **Test services with users as early as possible.** While the new system is being developed for use by all users, DoD is piloting it with certain types of travelers who have basic requests. DoD is following an industry best practice of launching systems earlier in their development, even when not all aspects may be fully automated. This will enable the team to improve the system based on real-world usage information.

18-F-1517//1355

3. **Use commercial cloud software services when possible, but be wary of commercial solutions that require extensive customization.** The modernized Defense travel system is being delivered using a commercial software-as-a-service travel tool, allowing DoD to avoid an unnecessary custom software development project. This is a best practice to follow when the commercial solutions require minimal customization to meet the government's needs. The DoD is seeking to avoid custom configuration requests for this service as much as possible, understanding that the expense and difficulty of such customizations often negate the benefits of using commercial services, and can lead to vendor lock-in.

4. **Modernization efforts should have clearly defined objectives.** If the success criteria above are met, this will enable the DOD to achieve the three main goals of modernizing the DTS: 1) Provide users a better customer experience, 2) increase the volume of trips, travelers and trip types processed with the system, and 3) save the Federal Government money. By clearly defining the strategic objectives of the effort, the delivery team can stay focused on what's important. In the absence of such a strategy, technical and policy constraints can drive product decisions.

18-F-1517//1356

Identifying Security Vulnerabilities in Department of Defense Websites – Hack the Pentagon

The Challenge

The Department of Defense (DoD) spends billions of dollars every year on information security. However, the DoD had not yet taken advantage of a "bug bounty" approach to identifying security vulnerabilities that has gained traction in the private sector.

In this "bug bounty" approach, private citizens and organizations are invited to probe specific services for potential security vulnerabilities, and are rewarded for qualifying vulnerabilities they uncover and responsibly disclose to the sponsoring organization. In this way, private citizens are provided a legal way to disclose potential vulnerabilities without fear of retaliation or prosecution, and are given an incentive for doing so. Private sector companies have successfully used this approach to improve the security of their systems. Despite this technique's acceptance as an industry best practice, the government had not attempted such an initiative before.

Project Impact Summary

- In January 2016, the Digital Service team at DoD (Defense Digital Service) got approval for the Hack the Pentagon program, inviting private citizens to find and get rewarded for uncovering vulnerabilities in its information security system.
- This "bug bounty" approach mirrors that used by companies like Facebook and Twitter to catch more vulnerabilities and cost-effectively improve security.
- DoD contracted HackerOne – a well-known bug bounty platform startup with a strong reputation in the hacker community – to run the program.
- The digital services team, in conjunction with the existing vendors, worked in near real-time to fix security flaws as they were disclosed.
- The program led to the resolution of 138 previously unidentified vulnerabilities and cost $150,000. Contracting an outside firm to do a similar audit would have cost an estimated $1M and possibly still would not have provided the same security coverage.
- In June, the Secretary of Defense announced that DoD would run a persistent bug bounty program, and efforts are being made to share the practice with other agencies. There are also additional bug bounties the DoD will be running through the month of December.

18-F-1517//1357

The Solution

On April 18, 2016, the DoD, supported by the USDS' Defense Digital Service team, launched the first bug bounty in the history of the Federal Government. This innovative effort adopted from the private sector provided authorization to security researchers – "hackers" – to attempt to hack limited public-facing DoD systems and report vulnerabilities in exchange for financial rewards. This crowdsourced solution used the talent of over a thousand individuals, 250 of whom submitted at least one vulnerability report. Of these, 138 vulnerabilities were determined to be legitimate and unique. These had escaped notice from previous penetration tests DoD conducted. Using this information, DoD resolved all of the vulnerabilities.

While the program was underway, the Defense Digital Service team held daily calls with all agency stakeholders for everyone's situational awareness in regards to bounty activities. There was also a pre-determined escalation process in place to follow in case of an immediate, critical need for defensive action against out-of-scope activity.

For the first challenge, the DoD contracted with HackerOne, an experienced administrator of bug bounty programs that performs services for companies such as Yahoo, Square, and Twitter. This strategy worked well for several reasons: HackerOne already had a strong reputation and relationship with the hacker community, they could quickly sub-contract a private background check firm, they receive and triage vulnerability reports, and they are able to allocate payouts for qualifying bounties. Using a third party platform also served to quell any concerns of hackers about providing personal information to the DoD as part of a larger effort to create a hacker database.

The cost of the program was $150,000. DoD estimates hiring an outside firm to perform a comparable security audit and vulnerability assessment would have cost more than $1 million.

18-F-1517//1358

In early June, Secretary of Defense Ash Carter announced his plan to launch a persistent DoD Bug Bounty program to continue to allow hackers to be paid for discovering security flaws in specific DoD websites, applications, binary code, networks, and systems. To make this possible, he had the Defense Digital Service take on three initiatives: run more bug bounty programs for other DoD components in 2016; develop a Vulnerability Disclosure Policy that would firmly and clearly express that hackers are acting legally when they surface DoD vulnerabilities; and provide guidance for the future acquisition of services like those provided by HackerOne.

To date, two new bug bounty programs are in the planning stages. The disclosure policy has been drafted, circulated, and is on track for release by the end of 2016. Acquisition guidance is in progress. The contract with HackerOne has been renewed, and is a model for future contracts not just at DoD, but government-wide. Altogether, these efforts will help the Defense Digital Service work with interagency teams to advise on implementing similar bug bounty programs. There will also be a "Government Only" day for agency stakeholders to gather and gain insight on Hack the Pentagon's model of success.

Success Criteria

Success Criteria	Status
Engage the hacker community.	Complete. 1,400 Registered Participants

18-F-1517//1359

Success Criteria	Status
Identify and fix previously unknown security vulnerabilities.	Complete. 138 vulnerability reports were determined to be legitimate, unique and actionable for remediation. DoD fixed all vulnerabilities identified.
Resolve vulnerabilities at a cost lower than would be possible with other methods.	Complete. The total contract cost was $150,000, with approximately half of this paid as bounties to participants. With 138 actionable vulnerability reports, that equates to less than $1,100 per vulnerability. DoD estimates it would have cost $1M for an outside firm to perform a similar security audit.

Milestones

- January 2016: Hack the Pentagon program approved.
- March 2016: Contract signed to start the program.
- April 2016: Challenge start date and bounty start date.
- May 2016: Bounty end dates.

The Process and Lessons Learned

1. **Provide a method for outside individuals to responsibly disclose security vulnerabilities.** Many private citizens have an interest in uncovering security issues. Private sector companies often provide such individuals a legal, secure way to disclose vulnerabilities without fear of retaliation or prosecution. Hack the Pentagon has shown that the "bug bounty" approach can work well for the government. Even if there is no active bug bounty program, providing researchers a way to provide responsible disclosure of vulnerabilities could yield results.

2. **Ensure the agency is prepared to remediate vulnerabilities as they are discovered, in near real-time.** DoD took the important step of putting a team

18-F-1517//1360

on standby that could implement fixes to the vulnerabilities as they were disclosed. Being able to quickly address issues helped ensure no malicious activity could take place.

3. **Involve stakeholders early.** Running a new type of program in government can be complicated. The Defense Digital Service team worked closely with the DoD Office of General Counsel to resolve legal questions around bug bounty payments, participant background checks, and whether bounties could be paid to U.S. Government personnel.

18-F-1517//1361

Section 3

Other USDS Initiatives

18-F-1517//1362

Hiring Top Technical Talent

The Challenge

In order to deliver on the mission of transforming the country's most important digital services, the Federal Government needs an infusion of modern software engineering, design, and product management skills. As demonstrated in earlier sections of this report, pairing individuals with these skills with dedicated civil servants across the Federal Government can dramatically accelerate modernization efforts on major IT acquisition projects.

However, hiring individuals with these skills has been challenging for the Federal Government for several reasons:

- It is difficult to attract highly qualified applicants to apply for government technology positions.
- The Federal Government often provides a candidate experience that is not competitive with the private sector in terms of timeline, ease of application, and frequent communication of application status.
- It is challenging to properly evaluate these highly specialized and technical skills in order to select the most qualified individuals from among all applicants.

One of the early priorities of the USDS was to build a robust recruitment and hiring program that could address these challenges.

Project Impact Summary

- It is difficult to attract highly qualified applicants from the private sector to apply for government technology positions, as the technology industry is one of the most competitive in the world.
- USDS partnered with OPM to secure the tools necessary to recruit and hire the country's brightest technical talent.
- Mirroring technology industry best practices, USDS built an experienced recruiting team who sources software engineering, product management, and design professionals from industry.
- USDS provides candidates with an easy application process and a fast timeline for hiring decisions, averaging 34 business days from application to conditional offer.

18-F-1517//1363

- USDS hiring process has a satisfaction score of 4.5 or greater (out of 5.0) from among all finalists, including those who did not receive offers.
- USDS uses subject matter experts to evaluate specialized skills.
- USDS has shortened the personnel security process from 67 days to 20 days.
- USDS reached its goal of recruiting 200 digital service experts by the end of 2016, ahead of schedule.

The Solution

USDS partnered with OPM to secure the tools necessary to recruit and hire the country's brightest technical talent. Using these tools, we created a recruiting and hiring operation that draws on several private sector best practices.

- **Engage in Targeted Recruiting Activities**. Mirroring private sector best practices, USDS has built an experienced recruiting team tasked with identifying and encouraging a diverse set of qualified applicants to apply for digital service positions. Specific tactics include targeted outreach to technology and design professionals (including those who are not currently seeking a new job), events, roundtables, and building a network of influencers who can validate the importance and professional respectability of the USDS' public service mission.

- **Focus on Candidate Experience**. The USDS hiring process puts a premium on providing a high quality candidate experience that is competitive with the private sector. Specifically, the USDS aims to provide candidates with an easy application process (currently delivered via the website), a fast timeline for hiring decisions (targeting 15 business days from application to conditional offer for qualified applicants), and good visibility into the process and application status.

  USDS measures its effectiveness by asking all candidates who complete the hiring process to complete a satisfaction survey, and target a satisfaction score of 4.5 or greater (out of 5.0) from among all finalists (including both those who receive offers and those who do not).

- **Use Subject Matter Experts to Evaluate Specialized Skills.** Evaluating applicants with highly specialized skills is a challenging practice that requires subject matter expert involvement at every stage. USDS has fully embraced the use of such experts in the hiring process. Each candidate for the USDS is evaluated by a panel of engineers, designers and product managers who themselves possess the desired specialized skills. By ensuring that applicants are evaluated by technical specialists within their own discipline, the process ensures

18-F-1517//1364

that individuals selected for USDS roles have the digital expert skills that are required to improve government technical services.

This hiring program is run centrally from the USDS headquarters unit inside OMB, so that all chartered USDS teams can benefit from a dedicated recruiting operation and a standardized, rigorous selection process.

Success Criteria	Status
Hire 200 Digital Service Experts by end of 2017	On track to meet target ahead of schedule. 196 Digital Service Experts hired as of September 2016.
Days from Application to Conditional Offer = 15 business days	In progress. Time reduced from 55 days in Q4 2015 to 34 days in Q3 2016.
Day from Conditional Offer to Final Offer (personnel security process) = 16 days	In progress. Time reduced from 67 days in Q4 2015 to 20 days in Q3 2016.
Candidate Satisfaction Score for going through the hiring process is 4.5 (or above) out of a scale from 1 to 5 (5 being the most satisfied)	On track. Average candidate satisfaction since Q4 2015 is greater than 4.5.

18-F-1517//1365

Transforming Federal IT Procurement

The Challenge

Government procurement cycles do not keep pace with fast-changing technology and user needs. This is largely due to a reliance on waterfall development methods where requirements are defined and documented in full detail before any design, development or user testing can take place. When tied to inflexible contracts, this approach makes it very difficult to build an easy to use, effective digital service. Adapting patterns and best practices from private industry will allow the Federal Government to deliver products faster, cheaper, and at higher quality.

Project Impact Summary

- The USDS procurement team has launched several projects to help the Federal Government enter into better, more agile contracts and buying decisions.
- The objective is not only to change the way IT services and products are acquired, but to model new procurement processes for the government at large.
- During a discovery sprint, the USDS team made recommendations for modernizing SAM.gov, the system businesses use to receive contracts and grants from the Federal Government.
- The GSA has accepted the recommendation to move SAM.gov to a Common Services Platform, allowing developers to make speedier improvements to the existing system, automate more services, and increase security.
- USDS also advised SBA to consolidate certification systems for small businesses seeking government contracts. SBA has since moved to a modern technology stack, and will soon process all certifications through certify.sba.gov.
- In October 2015, USDS and OFPP launched the Digital IT Acquisition Professional Training (DITAP) program, piloting a course that successfully taught federal contracting professionals material relevant to digital services procurement.
- USDS and OFPP are now working to transition this program to GSA and other Federal Government agencies.
- Also in partnership with OFPP, USDS developed the TechFAR Handbook, and the TechFAR Hub, to advise all federal agencies on how to adopt more flexible acquisition practices.

18-F-1517//1366

The Solution

USDS has a dedicated acquisition team working to improve the government technology marketplace and to help the government make better buying decisions. The USDS procurement team has launched several solutions since its inception and continues to evaluate new potential solutions.

System for Award Management (SAM.gov)

In order for businesses to receive a contract or grant from the government, they are required to register in the General Services Administration's (GSA) System for Award Management (SAM.gov). However, because the process is so cumbersome, many businesses are discouraged from engaging with the government. The USDS and GSA completed a two-week discovery sprint in March 2016 to define what a successful SAM.gov modernization would look like. This included evaluating the technology, business processes, and the customer experience underlying SAM and the related Integrated Award Environment.

USDS' recommendations from the discovery sprint included:

- **Shift from Process to Product.** In order to develop and ship such a large solution, the work must be centered around the idea that it is delivering a federal-wide product capable of meeting the demands and objectives of various and competing end user needs.
- **Invest in the Team.** Rather than hiring external experts, or bringing on other teams, GSA should make an investment in and prioritize comprehensive and frequent training for all roles within its Integrated Award Environment, from management to external stakeholders to contracting officers.
- **Empower a New Team Culture.** The unified team has the potential to deliver a powerful digital service by adopting a culture that embraces change, challenges the status quo, and does not accept anything less than excellence. The ideal team is self-motivated to look at everything as an opportunity to solve end users' problems.
- **Deliver. Deliver. Deliver.** The main benefit for adopting an agile development methodology is the ability to accelerate product delivery. Leadership must dissolve any fears of failure that create hesitancy when making a change to a product—whether it's prototypes, beta versions, or enhancements. The team has universally expressed a willingness to move to continuous integration, rapid delivery model, and USDS provided a 6-month plan for this transition.

18-F-1517//1367

- **Migrate to a Secure, Robust Services Platform.** The SAM.gov environment is transitioning to a Common Service Platform that will allow applications to be built on top of an infrastructure layer. Adopting continuous integration, implementing the "DevOps" practice of integrating system operations with application development teams and processes, and establishing protocols for a multi-vendor environment to implement changes on the new platform would speed improvements. In addition, there should be a drive to automate services and provide real-time data, such as TIN validation. To improve security, USDS recommended SAM.gov implement host segmentation and network security controls for restricting access to sensitive data on the Secure FTP service. Other key areas of opportunity recommended to improve the basic platform include open-source, standardization, and implementing a mitigation strategy for DDoS protection aligned with the public release of services on the Common Service Platform (CSP).

GSA has accepted the recommendations and is in the process of making nearly all of the changes. They have already restructured their team based on functions and are working cohesively in a team based environment.

Small Business Certifications

It is part of the mission of the Small Business Administration to expedite small businesses' access to government contracts. Better utilization of the 8(a) Business Development, Women-Owned Small Business (WOSB), HUBZone, and Service Disabled Veteran Owned Small Business Programs would serve this mission.

In early 2015, SBA asked the USDS to help it modernize and consolidate the systems that power these certification programs. After USDS personnel conducted an initial technical evaluation, the USDS procurement team assisted SBA in developing a contract to create a modern system using the best practices described in the Digital Services Playbook. SBA has since awarded an agile software development contract for revamping these certification processes as part of the SBAOne project.

In just 5 months following the award of the contract, SBA moved to a modern technology stack, hosted on flexible public cloud infrastructure, and launched an eligibility service in December 2015 for the WOSB program. This release was shortly followed by the successful launch of the modernized Woman-Owned Small Business certification system in March 2016 on certify.SBA.gov. Work is underway for the modernization of the 8(a) certification program, for a release planned in early 2017. Eventually all SBA Certifications will be processed through Certify.SBA.Gov.

18-F-1517//1368

Digital IT Acquisition Professional Training (DITAP)

Helping the government become smarter buyers requires the establishment of a specialized and educated procurement workforce that understands the digital and IT marketplace, utilizes best practices for IT purchasing, and capitalizes on the power of the government acting as a single purchasing entity and the economies of scale this provides. To achieve this, the USDS and the Office of Federal Procurement Policy (OFPP) have partnered to develop a digital IT acquisition professional community (DITAP).

The first component of this community was a training and certification program for contracting officers. USDS and OFPP posted a prize competition on Challenge.gov in May 2015 to develop the Digital Service Contracting Professional Training and Development Program for the Federal Government. As a part of this process, USDS and OFPP held a Reverse Industry Day where 70 representatives from vendors familiar with agile software development techniques, system integrators, collegiate entities, and training developer came together to confirm that the specific training did not yet exist and confirm that the Challenge.gov platform would be an effective path forward in developing the training. In all, 23 submissions were received, 3 finalists provided mock classroom presentations of their content and assessment plan, and by October 2015, the final winner began its finalized 6-month course with the first class of 30 Contracting Professionals from 20 federal agencies.

Over the 6 months, the attendees completed 11 days of classroom training on agile software development methodology, cloud hosting, and the "DevOps" practice of integrating system operations with application development teams and processes. The attendees completed 120 hours of self-directed learning and webinars, heard from 10 guest speakers, supported 6 live digital assignments, and completed a final capstone assessment of skills. Since the course ended in March 2016, 6 participants received promotions or changed job roles to take on IT work, 12 participants were assigned digital service acquisition work or are working with an agency digital service team, and two were named agency Acquisition Innovation Advocates. 90% of the 28 graduates felt they were ready to conduct digital service acquisitions in their agency. USDS and OFPP are restructuring the next round of implementation based on these results. The second class began in July 2016.

USDS and OFPP are currently training Federal Acquisition Institute (FAI) facilitators on how to conduct the program, for transfer of responsibilities in FY17. In addition, USDS and OFPP are finalizing the Federal Acquisition Certification in Contracting (FAC-C) Digital Service certificate program requirements and encouraging the development of similar training programs for government Contracting Officer Representatives and Project Managers. The long-term goal is for any federal training institution to be able to

18-F-1517//1369

use and update the course material in an open source manner to create their own development program without incurring the cost of content.

Success Criteria	Status
60 Contracting Officers trained in digital service acquisition.	In progress. 28 completed pilot. 30 started next round in July 2016

TechFAR Handbook

In the Government, digital services projects too often fail to meet user expectations or contain unused or unusable features. Several factors contribute to these outcomes, including, overly narrow interpretations of what is allowed by acquisition regulations. The Office of Federal Procurement Policy, with the assistance of the USDS, developed the TechFAR to highlight flexibilities in the Federal Acquisition Regulation (FAR) that can help agencies implement "plays" in the Digital Services Playbook.

The TechFAR is a handbook that describes relevant FAR authorities and includes practice tips, sample language, and a compilation of FAR provisions that are relevant to adopting an agile style of software development as the primary means of delivering software solutions. Agile software development is a proven commercial methodology characterized by incremental and iterative processes where releases are produced in close collaboration with the customer. The TechFAR facilitates a common understanding among agency stakeholders of the best ways to use acquisition authorities to maximize the likelihood for success in agile contracts and there is nothing prohibitive in the Federal Acquisition Regulations for adopting these methods and re-engineering contracts to support delivery of quality products. This handbook is a living document; users are urged to provide feedback, share experiences, and offer additional strategies, practice tips, policies, or contract language that may be used to assure that IT acquisitions achieve their desired results.

USDS also released the TechFAR Hub on GSA's Acquisition Gateway. The TechFAR Hub is designed to advise all federal agencies on how to implement best practices, as described in the digital service playbook and TechFAR, and as a community space for digital service practitioners.

18-F-1517//1370

Supporting the Development of Federal Shared Services

Shared technology platforms and services have the potential to simplify government products, increase consistency, reduce development costs, and eliminate duplication. Security also benefits by focusing resources on a smaller number of key components.

USDS is uniquely positioned to support the development of these shared services, because it works across many agencies and has visibility into many of the government's digital service development efforts. This insight enables USDS to invest in developing and promoting reusable platforms and services.

Project Impact Summary

- USDS supports the development of shared technology platforms and services because they have the potential to simplify government products, increase consistency, and reduce development costs.
- In May 2016, a USDS and 18F team began implementation work on Login.gov, a service that will provide a secure and user-friendly login process for multiple government digital services. Login.gov is currently being integrated with its first agency customer.
- Many government digital services are siloed under unique brands and programs, leading agencies to spend time and money redesigning common digital components such as buttons, forms and search bars. In September 2015, USDS and 18F released the U.S. Web Design Standards, a set of components that agencies can adopt to provide their users a consistent, high quality online experience while reducing the chance of duplicative work. Moving forward, GSA will continue to develop the Standards. Since its release, the standards have been downloaded over 17,000 times.

Login.gov Consumer Identity Platform

Many consumer-facing government digital services require individuals to create user accounts in order to access the service. The USDS has helped several agencies implement such systems, including at USCIS, CMS, SBA and IRS. Many more agencies have already implemented their own solutions. Despite several earlier attempts to build a common identity management platform, no such platform has been widely adopted.

18-F-1517//1371

Providing a secure and user-friendly login process for the government's digital services would improve the experience of interacting with government services, and help agencies implement digital services faster and more securely. To that end, the USDS and the General Service Administration's 18F are working iteratively with a team of technologists from across the Federal Government to build a platform for users who need to log in to government services. The team is coordinating with the Federal Acquisition Service, the Office of Management and Budget, and the National Institute of Standards and Technology on the specifics of the platform.

To build the Login.gov platform, the team is using modern, user-friendly, strong authentication and effective identity proofing technology. The project builds off of the hard work that was already done to create and implement the Connect.gov pilot, an earlier project with similar goals. The team is also using lessons learned from our counterparts in the UK who built GOV.UK Verify. More specifically, the team will accomplish these goals by:

- Creating a simple, elegant way for the public to verify their identity, log in to federal government websites, and, if necessary, recover their account
- Building experiences, processes, and infrastructure that will use the latest available technology to safeguard all user data
- Delivering software that will allow government developers to integrate it within hours, not weeks
- Iteratively improving the system throughout its lifetime
- Preserving privacy including mitigating risks and adhering to federal privacy guidelines
- Following security best practices including implementing easy-to-use multi-factor authentication

The team has identified the first agency to adopt this shared platform, and is in talks with several additional agency customers to be the second adopter early in 2017. Based on the success of the first two initial adopters, the team will scale out the adoption in 2017.

U.S. Web Design Standards

When members of the public access government services online, they're often met with confusing navigation systems, conflicting visual brands, and inconsistent interaction patterns — all factors that can erode trust in our government's services.

18-F-1517//1372

A snapshot of buttons across government websites

Recognizing the necessity of consistent, easy-to-use design, many agencies have started creating their own design patterns and user interface (UI) toolkits, but their efforts are often duplicative. Because many digital services are siloed under unique brands and programs, the Federal Government runs the risk of spending time and money reinventing the wheel — that is, recreating common patterns such as buttons, forms, and search bars that already exist. What's more, creating pattern libraries and toolkits is a time- and labor-intensive process, and one not all agencies have the resources to support.

Designers and developers at USDS and 18F teamed up to address the need for consistent, accessible design components. Together, they created the Draft U.S. Web Design Standards (the "Standards"), a set of open source UI components and a visual style guide that agencies can use to create consistent online experiences. The Standards, which launched in September 2015, follow industry-standard accessibility guidelines and draw on the best practices of existing style libraries and modern web design. To offer the highest-quality product, the Standards team makes frequent updates to introduce new features, fix bugs, provide clearer documentation, and more.

Agencies using the Standards enjoy several distinct benefits. Not only are they providing an enjoyable, consistent user experience, but they're also saving design and development time that can be dedicated to other projects. Using the Standards, a team can build a site quickly and with minimal effort, allowing their agency to communicate its message more effectively.

18-F-1517//1373

Moving forward, GSA's 18F team will continue to develop the Standards.

Success Criteria	Status
Overall Goal: Begin implementation of at least one outstanding common platform by end of 2016.	Complete. Implementation of shared login platform began in May 2016. Draft U.S. Web Design Standards released September 2015.
Sub-Goal: Draft U.S. Web Design Standards available for agency use.	Complete. Initially released in September 2015, they include an online style guide and downloadable software package. The standards have been downloaded more than 17,000 times. As of September 2016, more than 78 people have contributed to the Standards' code base, and more than 200 people have participated in conversations on the Standards' GitHub repository. The Standards team welcomes outside recommendations and contributions, which help drive the project's process forward.
Sub-Goal: At least three agencies have adopted a shared login service.	Incomplete. Development of an interagency login system is in progress, but it is not in use yet. Initial agency customer identified.

Milestones

Web Design Standards

- September 2015: Draft U.S. Web Design Standards released

Consumer Identity Platform

- December 2015: Identity sprint completed

18-F-1517//1374

- January 2016: Research starts
- May 2016: Implementation begins

18-F-1517//1375

Exhibit 37

U.S. tells Arkansas to delete files on voter data

By Bill Bowden , Brian Fanney twitter
This article was published today at 4:30 a.m.

0

Comments (8) Font Size

Arkansas voter data provided to President Donald Trump's voter-fraud commission is headed for the trash days after it was submitted.

According to an email exchange obtained Wednesday under the state Freedom of Information Act, Andrew Kossack, associate counsel for Vice President Mike Pence, asked officials in Secretary of State Mark Martin's office to delete from a federal server the voter data it submitted.

However, state officials could not access the server.

"We were unable to access the SAFE site again in order to pull down the file, pursuant to your request," wrote Peyton Murphy, assistant director of the state elections division, in a Monday email. "We understand that the file has not yet been accessed, but that it will expire 14 days from the time of the upload."

Kossack replied that the federal site would delete the file.

"I'll be back in touch with next steps," he continued. "Again, thank you for your submission, and my apologies for this inconvenience."

ADVERTISING

Arkansas submitted its data on July 5. It was the first state to submit data to the Presidential Advisory Commission on Election Integrity.

The SAFE site -- also known as the Safe Access File Exchange -- is at the heart of a lawsuit filed by the Washington, D.C.-based Electronic Privacy Information Center. The file exchange is run within the Department of Defense.

Kossack referred to the lawsuit in his email.

[EMAIL UPDATES: Get free breaking news alerts, daily newsletters with top headlines delivered to your inbox]

The Electronic Privacy Information Center contends that the commission failed to conduct a privacy information assessment -- required under the E-Government Act of 2002 -- before collecting the data using the Department of Defense system.

"The 'SAFE' URL, recommend by the Commission for the submission of voter data, leads election officials to a non-secure site," according to the Electronic Privacy Information Center.

"Regarding this website, Google Chrome states: 'Your connection is not private. Attackers may be trying to steal your information from [the site proposed by the Commission] (for example, passwords, messages, or credit cards).'"

In the initial request for information, dated June 28, Kris Kobach, vice chairman of the Presidential Advisory Commission on Election Integrity, noted that the commission wanted Arkansas data -- "if publicly available under the laws of your state" -- including names, addresses, dates of birth, political party affiliations, the last four digits of Social Security numbers "if available," voter history, voter status, felony convictions, information regarding voter registration in another state, military status and overseas citizen information.

The information submitted to the file exchange from Arkansas did not contain Social Security numbers, felony convictions, military status and driver's license numbers. Such information is not publicly available in Arkansas.

However, names, addresses, dates of birth, political party affiliations, voter history since 2008, registration status, email addresses and phone numbers -- were shared. The database does not say for whom someone voted -- only whether they voted.

The same Arkansas voter information that was released to the Trump administration has been provided about 200 times since January 2015 to various entities, Kelly Boyd, chief deputy secretary of state, told legislators and county clerks meeting Wednesday in Eureka Springs.

Those entities include states, organizations, political parties and Arkansas legislators, he told a crowd of about 100 at the Basin Park Hotel.

"We submit information every year to the state cross-check program, and we do that at no charge," Boyd said. "And we did that at no charge for this program."

"To be very clear on this, there was no sensitive information released, no Social Security numbers, no partials, no military data, no felon data, no data that you can't get out of the phone book."

Boyd said the data would reveal some voting information.

18-F-1517//1378

"They're going to know whether you voted R or D or O [optional] or N for nonjudicial in the primaries," said Boyd. "It would tell whether you voted E early, A absentee or P at the polls, back to 2008. ...

"I know there's been a lot of angst about that, and I'm sorry. I wish there hadn't been. This information is openly available. There are ways to make it not openly available. I'll work with you if you want to do that."

Gov. Asa Hutchinson told a group of high school students Monday that the state should not have provided any data to the Trump commission.

"I am not a fan of providing any data to the commission in Washington," Hutchinson said in response to a student's question.

"Even though it is publicly available information and anyone can get it -- all you have to do is file a Freedom of Information [Act] request to get the information -- I just don't want to facilitate the providing of that information to a federal database. I don't think that's helpful for us."

The governor spoke as Kossack and Arkansas secretary of state staff members were trading emails about deleting the Arkansas information.

Information for this article was contributed by The Associated Press.

Metro on 07/13/2017

Print Headline: U.S. tells state to delete files on voter data; But authorities in Arkansas unable to access federal site

Exhibit 38

DECLARATION OF MARC ROTENBERG

I, Marc Rotenberg, declare as follows:

1. I am President and Executive Director for the Plaintiff Electronic Privacy Information Center ("EPIC").

2. Plaintiff EPIC is a non-profit corporation located in Washington, D.C. EPIC is a public interest research center, which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has a particular interest in preserving privacy safeguards established by Congress, including the E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note), EPIC pursues a wide range of activities designed to protect privacy and educate the public, including policy research, public speaking, conferences, media appearances, publications, litigation, and comments for administrative and legislative bodies regarding the protection of privacy.

3. I am a member in good standing of the Bar of the District of Columbia (admitted 1990), the Bar of Massachusetts (1987), the U.S. Supreme Court (1991), the U.S. Court of Appeals—1st Circuit (2005), the U.S. Court of Appeals—2nd Circuit (2010), the U.S. Court of Appeals—3rd Circuit (1991) the U.S. Court of Appeals—4th Circuit (1992), the U.S. Court of Appeals—5th Circuit (2005), the U.S. Court of Appeals—7th Circuit (2011), the U.S. Court of Appeals—9th Circuit (2011), and the U.S. Court of Appeals—D.C. Circuit (1991).

4. I have taught Information Privacy Law continuously at Georgetown University Law Center since 1990.

5. I am co-author with Anita Allen of a leading casebook on privacy law.

6. In my capacity as President and Executive Director, I have supervised both EPIC's response to the Department's rulemaking and EPIC'S participation in all stages of litigation in the above-captioned matter.

7. The statements contained in this declaration are based on my own personal knowledge.

8. EPIC works with an Advisory Board consisting of nearly 100 experts from across the United States drawn from the information law, computer science, civil liberties and privacy communities.

9. Members of the EPIC Advisory Board must formally commit to joining the organization and to supporting the mission of the organization.

10. Members of the EPIC Advisory Board make financial contributions to support the work of the organization.

11. Members of the EPIC Advisory Board routinely assist with EPIC's substantive work. For example, members provide advice on EPIC's projects, speak at EPIC conferences, and sign on to EPIC amicus briefs.

12. In this matter, EPIC represented the interests of more than 30 members of the EPIC Advisory Board, who signed a Statement to the National Association of State Secretaries in Opposition to the Commission's demand for personal voter data.

Under penalty of perjury, I declare that the foregoing is true and correct to the best of my knowledge and belief.

Marc Rotenberg
EPIC President and Executive Director

Executed this 7th day of July, 2017

18-F-1517//1382

Exhibit 39

Trump election group backs away from its request for voter data after outcry

Commission on election integrity's 'repugnant' request for voter data prompted privacy concerns and numerous legal challenges

277

Andrew Gumbel in Los Angeles

Thursday 13 July 2017 05.00 EDT

The Trump administration is backing away from its extraordinary attempt to gather voters' personal information, following a barrage of legal challenges, an outcry from state officials, and a rash of voter registration cancellations by people concerned about their privacy.

ADVERTISING

Voting rights groups have filed at least six lawsuits in response to a letter sent out on 28 June by Kris Kobach, vice-chair of the presidential advisory commission on election integrity, asking state officials to provide names of the country's 150 million voters. In addition, the letter sought voters' addresses, social security numbers, voting histories, party affiliation, criminal histories, military status, and more.

18-F-1517//1384

Kobach has said the request is designed to help prevent fraudulent in-person voting. But his detractors say he is looking for a solution to a non-existent problem and suspect his true interest is in finding reasons to deny legitimate voters their rights, for partisan advantage.

Both Kobach and Trump have floated the notion that 3 to 5 million people voted illegally last November – a notion that has angered both Republican and Democratic election officials because there is no shred of evidence to support it.

> “ Trump’s voter fraud commission is a shameless white power grab
> Steven W Thrasher
>
> Read more

Kobach’s letter told states to comply with his request by 15 July, but the White House has already postponed that deadline pending a ruling from the Washington DC circuit court on one of the lawsuits. That ruling is not due until next week at the earliest.

The commission has also abandoned plans to store the information on a temporary Pentagon computer and promised to have a dedicated White House server ready to receive the data by next week.

Not one state – not even Kansas, where Kobach is secretary of state and in charge of elections – has agreed to comply fully with the request. Many have cited privacy concerns and other legal restraints. Only three states, Colorado, Missouri and Tennessee, have indicated any enthusiasm about complying. Many more have responded with fury, including Mississippi, whose Republican secretary of state memorably told Kobach to “go jump in the Gulf of Mexico”.

Advertisement

Maryland’s attorney general, Brian Frosh, called the request “repugnant”. “It appears designed only to intimidate voters,” he wrote, “and to indulge President Trump’s fantasy that he won the popular vote.”

According to the lawsuits filed by the Electronic Privacy Information Center (Epic), the American Civil Liberties Union (ACLU) and others, Kobach’s request sidestepped clear legal requirements on privacy protection – the issue that prompted the White House to hold off on its deadline.

The suits also accuse the commission of working at a constitutionally intolerable level of secrecy, and Kobach himself of blurring the legal lines between his position as vice-chair and his candidacy in next year’s Kansas gubernatorial election.

Epic’s complaint and call for a temporary restraining order, filed this month, denounced the proposed voter database as “unnecessary and excessive” and said the commission risked violating “the informational privacy rights of millions of Americans” and exposed the country’s electoral system to potential new forms of registration and voter fraud. To make the information gathered by the commission public, it added, would be “both without precedent and crazy”.

Donald and Melania Trump cast their votes in the 8 November 2016 presidential election. Photograph: Evan Vucci/AP

Two of the suits, by the ACLU and the Lawyers' Committee of Civil Rights Under Law, seek to postpone the presidential committee's next meeting, set for next Thursday, unless the White House discloses its communications about the meeting and opens it to the public.

Advertisement

Voting rights activists are hoping that the legal and political pressure will induce the White House to drop the data-gathering exercise altogether. "The program was ill conceived and poorly executed," Epic's president and executive director Marc Rotenberg said in a statement. "We expect the commission will simply announce that it has no intention, going forward, to ask the states for their voter records."

Some damage, however, has already been done, as election officials in at least four states – Arizona, Colorado, Florida and North Carolina – report receiving requests from hundreds of voters to cancel their registrations to protect their personal information.

Local voting officials were bombarded with email requests and phone calls after the Kobach letter became public. In some cases, the officials talked voters out of cancelling their registrations, arguing that the data was in the system already and they would only be damaging themselves. In other cases, voters said straight out they did not trust the presidential commission. One North Carolina voter said it "smells funny".

The voter response in Arizona appears to have triggered a change in policy. The secretary of state there initially said she would be withholding social security numbers, dates of birth and other identifying details but otherwise complying with the request. By the time she sent her official response, however, the line had changed to a flat no.

18-F-1517//1386

Exhibit 40

Arkansas Voter Registration Data

The Arkansas Secretary of State's Office provides three different statewide voter registration data files.

The first is the statewide Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted.

The second file contains the Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle. The older elections are incomplete since some counties did not enter voter results into the previously used VR databases. The Vote History file does not contain voters' names and therefore must be linked to the Voter Registration file by a unique Voter ID # found within each file.

The third file is a combination of the Voter Registration and Vote History files (VRVH).

- All files are ASCII text files with comma delimited, double quoted fields. This is commonly called comma-separated values format or .CSV format.
- Since there are about 1.6 million records in each, the files will not fit into an Excel spreadsheet.
- The VR file size is about 585 MB, the Vote History file size is about 402 MB, and the Combo file is about 1 GIG. Due to the file size no files can be sent via email.
- The cost per file is $2.50.
- The file(s) are available in CD format for pickup at the State Capitol Building or by mail. These files can also be placed on an FTP site if desired.

We are often asked the question, "Are there any restrictions on the use of this data?"
Currently there are no state laws that place restrictions on the use of data that we release. However, there are Federal and State laws that restrict some fields on the VR record from being released (Arkansas Code, Amendment 51§ 8(e)). These fields are never released and are never on any file that our office provides to the public.

To request a file you may complete the Data Request Form on the following page.

18-F-1517//1388

Data Request Form

Date: _____ Request taken by: _____

Contact Name: _____ Telephone: _____

Email Address: _____

Please check one of the following: Do you wish to...

Pick up the data ____ ***Have the data placed on your FTP site____***
Have the data mailed to the address below ____

Company: _____

Address: _____

City, State, Zip: _____

Data Requested, Comments and Instructions: _____

_____

_____

_____

_____

Number of Data Disk(s)/File(s)/Report(s) created: _____ created by: _____
Data Disk(s) filename(s): _____

_____

Please remit $2.50 for each enclosed Data Disk(s)/File(s)/Report(s)

Number of Data Disk(s)/File(s)/Report(s) created: _____ Total Cost:_____

Make Check or Money Order payable to: **Arkansas Secretary of State**

Mail payment to: ATTN: Data Request
Arkansas Secretary of State
State Capitol Bldg, Room 026
Little Rock, AR 72201

Any questions regarding this data should be reported to the Office of the Secretary of State at 1-800-247-3312 or via email at voterservices@sos.arkansas.gov .

18-F-1517//1389

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civ. Action No. 17-1320 (CKK)

[PROPOSED] ORDER GRANTING PLAINTIFF'S AMENDED MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

Upon consideration of Plaintiff's Amended Motion for a Temporary Restraining Order and Preliminary Injunction, Defendants' Opposition, Plaintiff's Reply, the hearings before this Court, the relevant legal authorities, and the record of this case as a whole;

The Court finds that Plaintiff is likely to succeed on the merits of its claims. The Court further concludes that Plaintiff has shown a likelihood of irreparable injury in the absence of injunctive relief, that the balance of equities favors Plaintiff, and that an injunction would be in the public interest. Given these considerations, the Court finds that injunctive relief is warranted in this case. It is, therefore,

ORDERED that Plaintiff's motion for a Preliminary Injunction is GRANTED. Defendants and their officers, agents, servants, employees, and attorneys, as well as any other persons who are in active concert or participation with the foregoing, are ENJOINED from collecting voter roll data from states and state election officials.

18-F-1517//1390

IT IS FURTHER ORDERED that Defendants immediately delete and disgorge any voter roll data already collected or hereafter received; and

ORDERED, in accordance with Fed. R. Civ. P. 65(c) and *NRDC v. Morton*, 337 F. Supp. 167, 169 (D.D.C. 1971), *aff'd on other grounds*, 458 F.2d 827 (D.C. Cir. 1972) (bonds for injunctive relief may be reduced when plaintiff initiates a public interest litigation), that this injunction shall be effective upon Plaintiff's giving of security in the amount of $10 by depositing that amount with the Clerk of Court.

Date: _____

Time: _____

_____
Colleen Kollar-Kotelly
United States District Judge

18-F-1517//1391

ORAL ARGUMENT NOT YET SCHEDULED

No. 17-5171

IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER
Plaintiff-Appellant,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,
Defendants-Appellees.

On Appeal from an Order of the
U.S. District Court for the District of Columbia

APPELLANT'S EMERGENCY MOTION TO EXPEDITE

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
CAITRIONA FITZGERALD
JERAMIE SCOTT
JOHN DAVISSON
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, D.C. 20009
(202) 483-1140
Counsel for Petitioner
Electronic Privacy Information Center

CERTIFICATE AS TO PARTIES, RULINGS AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), undersigned counsel for Appellant hereby provides the following information:

I. PARTIES AND *AMICI* APPEARING BELOW

The parties and amici who appeared before the U.S. District Court were:

1. Electronic Privacy Information Center, *Appellant*.
2. Presidential Advisory Commission on Election Integrity; Michael Pence, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; Kris Kobach, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; Charles C. Herndon, in his official capacity as Director of White House Information Technology; Executive Office of the President of the United States; Office of the Vice President of the United States; General Services Administration; United States Department of Defense; United States Digital Service; Executive Committee for Presidential Information Technology, *Defendants*.

II. PARTIES AND *AMICI* APPEARING IN THIS COURT

1. Electronic Privacy Information Center, *Appellant*.
2. Presidential Advisory Commission on Election Integrity; Michael Pence, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; Kris Kobach, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; Charles C. Herndon, in his official capacity as Director of White House Information Technology; Executive Office of the President of the United States; Office of the Vice President of the United States; General Services Administration; United States Department of Defense; United States Digital Service; Executive Committee for Presidential Information Technology, *Defendants*.

III. RULINGS UNDER REVIEW

The ruling under review in this case is United States District Court Judge Colleen Kollar-Kotelly's July 24, 2017, Order and Memorandum Opinion denying Appellant's Motion for a Temporary Restraining Order And Preliminary Injunction.

IV. RELATED CASES

Apart from the proceedings in the court below—*EPIC v. Presidential Advisory Comm'n on Election Integrity et al.*, No. 17-1320 (D.D.C. filed July 3, 2017)—this case has not previously been filed with this Court or any other court. Counsel is aware of the following cases qualifying as "related" under Circuit Rule 28(a)(1)(C):

- *ACLU v. Trump*, No. 17-1351 (D.D.C. filed July 10, 2017)
- *Lawyers' Committee for Civil Rights Under Law v. Presidential Advisory Comm'n on Election Integrity,* No. 17-1354 (D.D.C. filed July 10, 2017)
- *Public Citizen v. Army*, No. 17-1355 (D.D.C. filed July 10, 2017)
- *Common Cause v. Presidential Advisory Comm'n on Election Integrity*, No. 17-1398 (D.D.C. filed July 14, 2017)
- *Lawyers' Committee for Civil Rights Under Law v. Presidential Advisory Comm'n on Election Integrity,* No. 17-5167 (D.C. Cir. filed July 21, 2017)

Respectfully Submitted,

/s/ Marc Rotenberg
MARC ROTENBERG
EPIC President and Executive Director

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

PRELIMINARY STATEMENT

Appellant respectfully moves for expedited briefing and oral argument in the above-captioned appeal. Fed. R. App. P. 27; D.C. Cir. Rule 27; 28 U.S.C. § 1657(a) ("[E]ach court of the United States shall expedite the consideration of any action . . . for temporary or preliminary injunctive relief."). *EPIC v. Presidential Advisory Commission* presents the type of extraordinary circumstances that justify expedited consideration.

On July 3, 2017, EPIC sought a temporary restraining order and preliminary injunction to prevent the Presidential Advisory Commission on Election Integrity ("the Commission" or "PACEI") from collecting and aggregating state voter data (1) prior to completing and publishing a Privacy Impact Assessment ("PIA") as required by the E-Government Act of 2002, 44 U.S.C. § 3501 note, and the Federal Advisory Committee Act, 5 U.S.C. app. 2; and (2) prior to the resolution of EPIC's constitutional privacy claims. EPIC later amended its Motion on July 13, 2017. On July 24, 2017, the District Court denied EPIC's motion, concluding that "Defendants' collection of voter roll information does not currently involve agency action" as necessary for judicial review under the Administrative Procedure Act, 5 U.S.C. § 551 *et seq.*; Mem. Op. 1, Ex. 1. Almost immediately following the District Court's opinion in *EPIC v. Commission*, Commission Vice Chair Kris Kobach sent another letter to state election officials urging them to disclose personal voter data

to the Commission. Letter from Kris Kobach, Vice Chair, PACEI, to Alex Padilla, California Sec'y of State (July 26, 2017), Ex. 2. Absent expedited review of the District Court's Order, the Commission will be allowed to collect the personal data of the nation's voters without first conducting and publishing a Privacy Impact Assessment as required by law.

BACKGROUND

Appellant EPIC seeks expedited review of its appeal from the U.S. District Court for the District of Columbia's denial of EPIC's Motion for a Temporary Restraining Order and Preliminary Injunction, in which EPIC asked the Court to block the Commission from collecting and aggregating state voter data (1) prior to completing and publishing a Privacy Impact Assessment as required by the E-Government Act of 2002, 44 U.S.C. § 3501 note, and the Federal Advisory Committee Act, 5 U.S.C. app. 2; and (2) prior to the resolution of EPIC's constitutional privacy claims.

The Presidential Advisory Commission on Election Integrity was established by executive order on May 11, 2017. Exec. Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017), Ex. 3. The Vice President is named as the Chair of the Commission, "which shall be composed of not more than 15 additional members." *Id.* Additional members are appointed by the President, and the Vice President may select a Vice Chair of the Commission from among the members. *Id.* Vice President

Pence has named Kansas Secretary of State Kris Kobach to serve as Vice Chair of the Commission.

The Commission was asked to "*study* the registration and voting processes used in Federal elections." *Id.* (emphasis added). The Commission was further asked to identify "(a) those laws, rules, policies, activities, strategies, and practices that enhance the American people's confidence in the integrity of the voting processes used in Federal elections; (b) those laws, rules, policies, activities, strategies, and practices that undermine the American people's confidence in the integrity of the voting processes used in Federal elections; and (c) those vulnerabilities in voting systems and practices used for Federal elections that could lead to improper voter registrations and improper voting, including fraudulent voter registrations and fraudulent voting." *Id.*

Under the text of the Executive Order and the Charter of the Commission, the General Services Administration ("GSA") is designated as the "Agency Responsible for Providing Support" to the Commission. *Id.* sec. 7(a); Charter, Presidential Advisory Commission on Election Integrity at sec. 6. The GSA was specifically tasked with providing the Commission, *inter alia*, "administrative services," "facilities," "equipment" and "other support services as may be necessary to carry out its mission . . ." *Id.* The only derogation from the assignments of these responsibilities to the GSA is a provision which states that "the President's designee

will be responsible for fulfilling the requirements of subsection 6(b) of the FACA." *Id.*

There is no authority in the Executive Order or the Charter of the Commission to collect voter record information from state election officials.

Nonetheless, on June 28, 2017, Mr. Kobach undertook an unprecedented effort to collect detailed personal information on voters nationwide. He sent letters to election officials in all fifty states and the District of Columbia seeking:

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.

See, e.g., Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017) at 1–2, Ex. 4 ("Commission Letter"). The Commission Letter said that state officials should provide only "publicly available" information, but no attempt was made by the Commission to determine which state data was in fact "publicly available" or to comply with the various other requirements that typically attach to a request for state voter information, such as the designation of files, the payment of fees, the completion of forms, and the use of secure techniques to permit the transfer of sensitive personal data.

Mr. Kobach stated that he expected a response from the states by July 14, 2017—approximately ten business days after the date of the initial request.

On July 3, 2017, EPIC filed suit in U.S. District Court for the District of Columbia. *Electronic Privacy Information Center v. Presidential Advisory Commission on Election Integrity, et al.*, No. 17-1320 (D.D.C. July 24, 2017).

On July 7, 2017, a hearing was held before the District Court. *See* TRO Hr'g Tr., July 7, 2017, Ex. 5.

On July 10, 2017, the Commission suspended the data collection program. E-mail from Andrew Kossack, Designated Federal Officer, PACEI, to state election officials (July 10, 2017, 9:40 AM), Ex. 6. In a subsequent declaration from Kobach, the Commission stated (1) that it would suspend the data collection pending the Court's decision on this motion; (2) that the Commission had discontinued use of the military website to receive voter data; and (3) that the Commission would delete the data that had been received from the state of Arkansas. Third Kobach Decl., Ex. 7.

On July 13, 2017, pursuant to an Order of the District Court, EPIC filed an Amended Motion for a Temporary Restraining Order and Preliminary Injunction. Order, Ex. 8.

On July 24, 2017, the Opinion and Order of the District Court issued. Mem. Op., Ex. 1.

On July 26, 2017, Kobach sent another letter to the 50 states and the District of Columbia "to renew the June 28 request" and to urge state election officials to turn over state voter records to the Commission. *See, e.g.*, Letter from Kris Kobach, Vice Chair, PACEI, to Alex Padilla, Cal. Sec'y of State (July 26, 2017), Ex. 2. The July 26 letter raised new concerns about possible misuses of the personal data sought by the Commission, as well as uncertainty about the future handling of the data: "Once the Commission's analysis is complete, the Commission will dispose of the data as permitted by federal law." *Id.* at 2. For example, the July 26 letter does not indicate who will have access to the data collected, why the data is being collected, for what purposes the data will be used, how the data will be secured, whether a Privacy Act notice will be pursued, whether individuals will have the opportunity to "opt out" of the data collection, whether the data will be retained, or how any conclusions drawn from the "analysis" may be contested.

Such a collection of personal data by a federal agency is entirely contrary to the section 208 of the E-Government Act of 2002 which requires that any federal agency "initiating a new collection of information that (I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual" complete a Privacy Impact Assessment before initiating such collection. 44 U.S.C. § 3501 note.

The Privacy Impact Assessment would require the Commission to state:

> (I) what information is to be collected;
> (II) why the information is being collected;
> (III) the intended use of the agency of the information;
> (IV) with whom the information will be shared;
> (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
> (VI) how the information will be secured; and
> (VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the ''Privacy Act'').

Id. § 208 (b)(2)(B)(ii).

Given the sensitivity of voter data and the widely known fact that a foreign adversary targeted U.S. voter registration records, a Privacy Impact Assessment may have led to the conclusion that the Commission simply could not collect state voter record information as proposed. And a PIA would have triggered obligations under the federal Privacy Act that would have established procedural safeguards against adverse determinations arising from computer matching programs undertaken by a federal agency. Moreover, under the Federal Advisory Committee Act, the Appellees would have been required to make available the PIA to the public. 5 U.S.C. app. 2 § 10(b).

None of the Appellee agencies have conducted a Privacy Impact Assessment for the Commission's proposed collection of state voter data. None of the Appellee

agencies have ensured review of a PIA by any Chief Information Officer or equivalent official. The Commission has not made any PIA available to the public.

ARGUMENT

Appellant is entitled to expedited review as of right because the ruling under review is a denial of EPIC's motion for temporary and preliminary injunctions. 28 U.S.C. § 1657(a) ("[E]ach court of the United States shall expedite the consideration of any action . . . for temporary or preliminary injunctive relief."); Circuit Rule 47.2(a) ("[I]n an action seeking temporary or preliminary injunctive relief" the clerk must "prepare an expedited schedule for briefing and argument."). *Am. Bioscience, Inc. v. Thompson*, 269 F.3d 1077, 1084 n.8 (D.C. Cir. 2001) ("[U]nder 28 U.S.C. § 1657(a), the granting or denying of a preliminary injunction is the basis for an expedited appeal.").

EPIC is also entitled to expedited review because "good cause" exists for such treatment. 28 U.S.C. § 1657(a). "'Good cause' is shown if a right under the Constitution of the United States or a Federal Statute would be maintained in a factual context that indicates that a request for expedited consideration has merit." *Id.* To the extent that the Commission might evade the E-Government Act's Privacy Impact Assessment requirement by using non-GSA facilities to collect voter data, EPIC would face certain informational injury due to the non-disclosure of a PIA. This Court also has the discretion to grant expedited review if "delay will cause

irreparable injury and . . . the decision under review is subject to substantial challenge" or if "the public generally, or . . . persons not before the Court, have an unusual interest in prompt disposition." U.S. Court of Appeals for the D.C. Circuit, *Handbook of Practice and Internal Procedures* at 33 (Jan. 26, 2017).

This case presents the exactly the type of extraordinary circumstances that require expedited consideration. Absent expedited review, the Commission will be allowed to collect the nation's voter records without first undertaking a Privacy Impact Assessment, an obligation that should certainly attach to the personal information necessary to sustain the country's democratic institutions. Under 28 U.S.C. § 1657(a), this Court must expedite the review of Appellant's appeal.

I. Delay Will Cause Appellant Irreparable Injury

Any delay in resolution of this appeal will cause irreparable injury to EPIC. EPIC is entitled under the E-Government Act of 2002 to access, review, and disseminate a Privacy Impact Assessment prior to the Commission's collection and creation of a new system to collect personal voter data. The District Court held that the failure to produce the Privacy Impact Assessment imposes on EPIC "the very injuries meant to be prevented by the disclosure of information pursuant to the E-Government Act—lack of transparency and the resulting lack of opportunity to hold the federal government to account." Mem. Op. 16–17. *See also Pub. Citizen v. DOJ*, 491 U.S. 440, 447 (1989).

This injury is particular to EPIC because EPIC's mission is to "focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age." Mem. Op. 17. Absent resolution of the claims under the APA, E-Government Act, and Federal Advisory Committee Act, EPIC will be unable to fully "carry out its mission to educate the public regarding privacy issues." Mem. Op. 17. The Commission's failure to produce a Privacy Impact Assessment impairs EPIC's "programmatic activities—educating the public regarding privacy matters— . . . since those activities routinely rely upon access to information from the federal government." Mem. Op. 26.

II. The District Court's Opinion is Subject to Substantial Challenge

EPIC's appeal also presents a substantial challenge to the District Court's decision. The District Court held that the Commission and the Director of White House Information Technology ("DWHIT") were not "agencies," Mem. Op. 27, 32, relying on the "substantial independent authority" test that controls in FOIA cases. *Soucie v. David*, 448 F.2d 1067, 1073 (D.C. Cir. 1971); *see also Citizens for Responsibility & Ethics in Washington v. Office of Admin.*, 566 F.3d 219, 222 (D.C. Cir. 2009); *Armstrong v. Exec. Office of the President*, 90 F.3d 553, 558 (D.C. Cir. 1996) (citing *Meyer v. Bush*, 981 F.2d 1288 (D.C. Cir. 1993).

But the District Court was wrong to allow a FOIA test to govern the outcome of this case: this Circuit's precedents demonstrate that the term "agency" carries distinct meanings under the APA and the FOIA. *Compare Armstrong v. Bush*, 924 F.2d 282, 291 (D.C. Cir. 1991) (applying the APA to the National Security Council ("NSC") as an "agency"), *with Armstrong v. Exec. Office of the President*, 90 F.3d 553, 557–66 (D.C. Cir. 1996) (holding that the NSC is not an "agency" under the FOIA); *see id.* at 566 (The Court's holding under FOIA still left "the question [of] whether the NSC is an 'agency' within the meaning of that term as it is used in the APA. *See* 5 U.S.C. § 551(1) (agency defined as 'each authority of the Government of the United States')."). Nor has this Court ever held that a Presidential Advisory Commission is not subject to the APA or that a Presidential Advisory Commission would not be subject to Section 208 of the E-Government Act of 2002. EPIC's appeal thus represents a substantial challenge requiring the Court's immediate attention.

III. The Public has an Unusual Interest in Prompt Disposition

Finally, non-parties and the public generally also have an unusual and extraordinarily strong interest in a prompt disposition of this case. There are now 512 pages of public comments responding to the Commission's attempt to file personal voter data, the vast majority of which are opposed to the Commission's

proposed collection of state voter records. *See Presidential Advisory Commission on Election Integrity Resources*, The White House.[1]

The vast majority of states have also refused to turn over the voter data the Commission is seeking. *Forty-four States and DC Have Refused to Give Certain Voter Information to Trump Commission,* CNN (July 5, 2017).[2] California Secretary of State Alex Padilla stated on June 29, 2017, that "[t]he President's commission has requested the personal data and the voting history of every American voter–including Californians. As Secretary of State, it is my duty to ensure the integrity of our elections and to protect the voting rights and privacy of our state's voters." Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017).[3] On July 25, 2017, after the district court's ruling, Secretary Padilla reaffirmed that he would not comply with the Commission's request. Press Release, Secretary of State Alex Padilla Reaffirms California Will Not Comply with Kobach Commission

---

[1] https://www.whitehouse.gov/presidential-advisory-commission-election-integrity-resources (last visited July 27, 2017).
[2] http://www.cnn.com/2017/07/03/politics/kris-kobach-letter-voter-fraud-commission-information/index.html.
[3] http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/.

Voter Data Request (July 25, 2017).[4] Nebraska Secretary of State John Gale stated on July 6, 2017 that "I also have a concern about data privacy. I have no clear assurances about the security that this national database will receive. In light of the domestic and foreign attacks in 2016 on state voter registration databases, the commission will need to assure my office of a high level of security." Press Release, Sec. Gale Issues Statement on Request for NE Voter Record Information (July 6, 2017).[5] Arizona Secretary of State Michele Reagan said:

> I share the concerns of many Arizona citizens that the Commission's request implicates serious privacy concerns. [...] Since there is nothing in Executive Order 13799 (nor federal law) that gives the Commission authority to unilaterally acquire and disseminate such sensitive information, the Arizona Secretary of State's Office is not in a position to fulfill your request.
>
> [...]
> Centralizing sensitive voter registration information from every U.S. state is a potential target for nefarious actors who may be intent on further undermining our electoral process. [...] Without any explanation how Arizona's voter information would be safeguarded or what security protocols the Commission has put in place, I cannot in good conscience release Arizonans' sensitive voter data for this hastily organized experiment.

---

[4] http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-reaffirms-california-will-not-comply-kobach-commission-voter-data-request/.
[5] http://www.sos.ne.gov/admin/press_releases/pdf-2017/nr-20170707.pdf.

Letter from Michele Reagan, Arizona Sec. of State, to Kris Kobach, Vice Chair, PACEI (July 3, 2017).[6]

States are debating how to comply with the Commission's request while this appeal is pending. State election officials and their constituents have a strong, vested interest in the prompt resolution of this case so that the personal information of voters is protected.

Considering the need for the utmost expedition in this matter, Appellant proposes the following briefing schedule:

Appellant's Opening Brief	August 18, 2017
Appellees' Brief	September 15, 2017
Appellant's Reply Brief	September 22, 2017

Appellant has contacted Appellees' counsel, and they do not oppose this proposed briefing schedule.

CONCLUSION

For the foregoing reasons, Appellant respectfully requests that consideration of this matter be expedited, that the Court issue an order setting the above briefing schedule, and that the Court direct the Clerk to schedule oral argument on the earliest available date following the completion of briefing.

---

[6] https://assets.documentcloud.org/documents/3884344/Kobach-Response-Letter-DRAFT-1.pdf.

Respectfully Submitted,

/s/ Marc Rotenberg

Marc Rotenberg,
Alan Butler
Caitriona Fitzgerald
Jeramie D. Scott
John Davisson
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140
rotenberg@epic.org

Attorneys for Appellant EPIC

Dated: July 28, 2017

CERTIFICATE OF SERVICE

I, Marc Rotenberg, hereby certify that on July 28, 2017, I electronically filed the foregoing document with the Clerk of the Court for the United States Court of Appeals for the D.C. Circuit by using the CM/ECF system. The following participants in the case who are registered CM/ECF users will be served by the CM/ECF system:

Daniel Tenny
Email: daniel.tenny@usdoj.gov
U.S. Department of Justice
(DOJ) Civil Division, Appellate Staff
Firm: 202-514-2000
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Elizabeth J. Shapiro
Direct: 202-514-5302
Email: elizabeth.shapiro@usdoj.gov
Fax: 202-616-8470
U.S. Department of Justice
(DOJ) Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, DC 20530

Mark B. Stern, Attorney
Email: mark.stern@usdoj.gov
U.S. Department of Justice
(DOJ) Civil Division, Appellate Staff
Firm: 202-514-2000
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

/s/ Marc Rotenberg
MARC ROTENBERG

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6). The motion is composed in a 14-point proportional typeface, Times New Roman, and complies with the word limit of Fed. R. App. P. 27(d)(2)(A) and D.C. Circuit Rule 27(a)(2), because it contains 3,111 words.

/s/ Marc Rotenberg
MARC ROTENBERG

ORAL ARGUMENT NOT YET SCHEDULED

No. 17-5171

IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER
Plaintiff-Appellant,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,
Defendants-Appellees.

On Appeal from an Order of the
U.S. District Court for the District of Columbia

APPELLANT'S EMERGENCY MOTION TO EXPEDITE

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
CAITRIONA FITZGERALD
JERAMIE SCOTT
JOHN DAVISSON
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, D.C. 20009
(202) 483-1140
Counsel for Petitioner
Electronic Privacy Information Center

CERTIFICATE AS TO PARTIES, RULINGS AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), undersigned counsel for Appellant hereby provides the following information:

I. PARTIES AND *AMICI* APPEARING BELOW

The parties and amici who appeared before the U.S. District Court were:

1. Electronic Privacy Information Center, *Appellant*.
2. Presidential Advisory Commission on Election Integrity; Michael Pence, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; Kris Kobach, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; Charles C. Herndon, in his official capacity as Director of White House Information Technology; Executive Office of the President of the United States; Office of the Vice President of the United States; General Services Administration; United States Department of Defense; United States Digital Service; Executive Committee for Presidential Information Technology, *Defendants*.

II. PARTIES AND *AMICI* APPEARING IN THIS COURT

1. Electronic Privacy Information Center, *Appellant*.
2. Presidential Advisory Commission on Election Integrity; Michael Pence, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; Kris Kobach, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; Charles C. Herndon, in his official capacity as Director of White House Information Technology; Executive Office of the President of the United States; Office of the Vice President of the United States; General Services Administration; United States Department of Defense; United States Digital Service; Executive Committee for Presidential Information Technology, *Defendants*.

III. RULINGS UNDER REVIEW

The ruling under review in this case is United States District Court Judge Colleen Kollar-Kotelly's July 24, 2017, Order and Memorandum Opinion denying Appellant's Motion for a Temporary Restraining Order And Preliminary Injunction.

IV. RELATED CASES

Apart from the proceedings in the court below—*EPIC v. Presidential Advisory Comm'n on Election Integrity et al.*, No. 17-1320 (D.D.C. filed July 3, 2017)—this case has not previously been filed with this Court or any other court. Counsel is aware of the following cases qualifying as "related" under Circuit Rule 28(a)(1)(C):

- *ACLU v. Trump*, No. 17-1351 (D.D.C. filed July 10, 2017)
- *Lawyers' Committee for Civil Rights Under Law v. Presidential Advisory Comm'n on Election Integrity,* No. 17-1354 (D.D.C. filed July 10, 2017)
- *Public Citizen v. Army*, No. 17-1355 (D.D.C. filed July 10, 2017)
- *Common Cause v. Presidential Advisory Comm'n on Election Integrity*, No. 17-1398 (D.D.C. filed July 14, 2017)
- *Lawyers' Committee for Civil Rights Under Law v. Presidential Advisory Comm'n on Election Integrity,* No. 17-5167 (D.C. Cir. filed July 21, 2017)

Respectfully Submitted,

/s/ Marc Rotenberg
MARC ROTENBERG
EPIC President and Executive Director

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

PRELIMINARY STATEMENT

Appellant respectfully moves for expedited briefing and oral argument in the above-captioned appeal. Fed. R. App. P. 27; D.C. Cir. Rule 27; 28 U.S.C. § 1657(a) ("[E]ach court of the United States shall expedite the consideration of any action . . . for temporary or preliminary injunctive relief."). *EPIC v. Presidential Advisory Commission* presents the type of extraordinary circumstances that justify expedited consideration.

On July 3, 2017, EPIC sought a temporary restraining order and preliminary injunction to prevent the Presidential Advisory Commission on Election Integrity ("the Commission" or "PACEI") from collecting and aggregating state voter data (1) prior to completing and publishing a Privacy Impact Assessment ("PIA") as required by the E-Government Act of 2002, 44 U.S.C. § 3501 note, and the Federal Advisory Committee Act, 5 U.S.C. app. 2; and (2) prior to the resolution of EPIC's constitutional privacy claims. EPIC later amended its Motion on July 13, 2017. On July 24, 2017, the District Court denied EPIC's motion, concluding that "Defendants' collection of voter roll information does not currently involve agency action" as necessary for judicial review under the Administrative Procedure Act, 5 U.S.C. § 551 *et seq.*; Mem. Op. 1, Ex. 1. Almost immediately following the District Court's opinion in *EPIC v. Commission*, Commission Vice Chair Kris Kobach sent another letter to state election officials urging them to disclose personal voter data

to the Commission. Letter from Kris Kobach, Vice Chair, PACEI, to Alex Padilla, California Sec'y of State (July 26, 2017), Ex. 2. Absent expedited review of the District Court's Order, the Commission will be allowed to collect the personal data of the nation's voters without first conducting and publishing a Privacy Impact Assessment as required by law.

BACKGROUND

Appellant EPIC seeks expedited review of its appeal from the U.S. District Court for the District of Columbia's denial of EPIC's Motion for a Temporary Restraining Order and Preliminary Injunction, in which EPIC asked the Court to block the Commission from collecting and aggregating state voter data (1) prior to completing and publishing a Privacy Impact Assessment as required by the E-Government Act of 2002, 44 U.S.C. § 3501 note, and the Federal Advisory Committee Act, 5 U.S.C. app. 2; and (2) prior to the resolution of EPIC's constitutional privacy claims.

The Presidential Advisory Commission on Election Integrity was established by executive order on May 11, 2017. Exec. Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017), Ex. 3. The Vice President is named as the Chair of the Commission, "which shall be composed of not more than 15 additional members." *Id.* Additional members are appointed by the President, and the Vice President may select a Vice Chair of the Commission from among the members. *Id.* Vice President

Pence has named Kansas Secretary of State Kris Kobach to serve as Vice Chair of the Commission.

The Commission was asked to "*study* the registration and voting processes used in Federal elections." *Id.* (emphasis added). The Commission was further asked to identify "(a) those laws, rules, policies, activities, strategies, and practices that enhance the American people's confidence in the integrity of the voting processes used in Federal elections; (b) those laws, rules, policies, activities, strategies, and practices that undermine the American people's confidence in the integrity of the voting processes used in Federal elections; and (c) those vulnerabilities in voting systems and practices used for Federal elections that could lead to improper voter registrations and improper voting, including fraudulent voter registrations and fraudulent voting." *Id.*

Under the text of the Executive Order and the Charter of the Commission, the General Services Administration ("GSA") is designated as the "Agency Responsible for Providing Support" to the Commission. *Id.* sec. 7(a); Charter, Presidential Advisory Commission on Election Integrity at sec. 6. The GSA was specifically tasked with providing the Commission, *inter alia*, "administrative services," "facilities," "equipment" and "other support services as may be necessary to carry out its mission . . ." *Id.* The only derogation from the assignments of these responsibilities to the GSA is a provision which states that "the President's designee

will be responsible for fulfilling the requirements of subsection 6(b) of the FACA." *Id.*

There is no authority in the Executive Order or the Charter of the Commission to collect voter record information from state election officials.

Nonetheless, on June 28, 2017, Mr. Kobach undertook an unprecedented effort to collect detailed personal information on voters nationwide. He sent letters to election officials in all fifty states and the District of Columbia seeking:

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.

See, e.g., Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017) at 1–2, Ex. 4 ("Commission Letter"). The Commission Letter said that state officials should provide only "publicly available" information, but no attempt was made by the Commission to determine which state data was in fact "publicly available" or to comply with the various other requirements that typically attach to a request for state voter information, such as the designation of files, the payment of fees, the completion of forms, and the use of secure techniques to permit the transfer of sensitive personal data.

Mr. Kobach stated that he expected a response from the states by July 14, 2017—approximately ten business days after the date of the initial request.

On July 3, 2017, EPIC filed suit in U.S. District Court for the District of Columbia. *Electronic Privacy Information Center v. Presidential Advisory Commission on Election Integrity, et al.*, No. 17-1320 (D.D.C. July 24, 2017).

On July 7, 2017, a hearing was held before the District Court. *See* TRO Hr'g Tr., July 7, 2017, Ex. 5.

On July 10, 2017, the Commission suspended the data collection program. E-mail from Andrew Kossack, Designated Federal Officer, PACEI, to state election officials (July 10, 2017, 9:40 AM), Ex. 6. In a subsequent declaration from Kobach, the Commission stated (1) that it would suspend the data collection pending the Court's decision on this motion; (2) that the Commission had discontinued use of the military website to receive voter data; and (3) that the Commission would delete the data that had been received from the state of Arkansas. Third Kobach Decl., Ex. 7.

On July 13, 2017, pursuant to an Order of the District Court, EPIC filed an Amended Motion for a Temporary Restraining Order and Preliminary Injunction. Order, Ex. 8.

On July 24, 2017, the Opinion and Order of the District Court issued. Mem. Op., Ex. 1.

On July 26, 2017, Kobach sent another letter to the 50 states and the District of Columbia "to renew the June 28 request" and to urge state election officials to turn over state voter records to the Commission. *See, e.g.*, Letter from Kris Kobach, Vice Chair, PACEI, to Alex Padilla, Cal. Sec'y of State (July 26, 2017), Ex. 2. The July 26 letter raised new concerns about possible misuses of the personal data sought by the Commission, as well as uncertainty about the future handling of the data: "Once the Commission's analysis is complete, the Commission will dispose of the data as permitted by federal law." *Id.* at 2. For example, the July 26 letter does not indicate who will have access to the data collected, why the data is being collected, for what purposes the data will be used, how the data will be secured, whether a Privacy Act notice will be pursued, whether individuals will have the opportunity to "opt out" of the data collection, whether the data will be retained, or how any conclusions drawn from the "analysis" may be contested.

Such a collection of personal data by a federal agency is entirely contrary to the section 208 of the E-Government Act of 2002 which requires that any federal agency "initiating a new collection of information that (I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual" complete a Privacy Impact Assessment before initiating such collection. 44 U.S.C. § 3501 note.

The Privacy Impact Assessment would require the Commission to state:

> (I) what information is to be collected;
> (II) why the information is being collected;
> (III) the intended use of the agency of the information;
> (IV) with whom the information will be shared;
> (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
> (VI) how the information will be secured; and
> (VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the ''Privacy Act'').

Id. § 208 (b)(2)(B)(ii).

Given the sensitivity of voter data and the widely known fact that a foreign adversary targeted U.S. voter registration records, a Privacy Impact Assessment may have led to the conclusion that the Commission simply could not collect state voter record information as proposed. And a PIA would have triggered obligations under the federal Privacy Act that would have established procedural safeguards against adverse determinations arising from computer matching programs undertaken by a federal agency. Moreover, under the Federal Advisory Committee Act, the Appellees would have been required to make available the PIA to the public. 5 U.S.C. app. 2 § 10(b).

None of the Appellee agencies have conducted a Privacy Impact Assessment for the Commission's proposed collection of state voter data. None of the Appellee

agencies have ensured review of a PIA by any Chief Information Officer or equivalent official. The Commission has not made any PIA available to the public.

ARGUMENT

Appellant is entitled to expedited review as of right because the ruling under review is a denial of EPIC's motion for temporary and preliminary injunctions. 28 U.S.C. § 1657(a) ("[E]ach court of the United States shall expedite the consideration of any action . . . for temporary or preliminary injunctive relief."); Circuit Rule 47.2(a) ("[I]n an action seeking temporary or preliminary injunctive relief" the clerk must "prepare an expedited schedule for briefing and argument."). *Am. Bioscience, Inc. v. Thompson*, 269 F.3d 1077, 1084 n.8 (D.C. Cir. 2001) ("[U]nder 28 U.S.C. § 1657(a), the granting or denying of a preliminary injunction is the basis for an expedited appeal.").

EPIC is also entitled to expedited review because "good cause" exists for such treatment. 28 U.S.C. § 1657(a). "'Good cause' is shown if a right under the Constitution of the United States or a Federal Statute would be maintained in a factual context that indicates that a request for expedited consideration has merit." *Id.* To the extent that the Commission might evade the E-Government Act's Privacy Impact Assessment requirement by using non-GSA facilities to collect voter data, EPIC would face certain informational injury due to the non-disclosure of a PIA. This Court also has the discretion to grant expedited review if "delay will cause

irreparable injury and . . . the decision under review is subject to substantial challenge" or if "the public generally, or . . . persons not before the Court, have an unusual interest in prompt disposition." U.S. Court of Appeals for the D.C. Circuit, *Handbook of Practice and Internal Procedures* at 33 (Jan. 26, 2017).

This case presents the exactly the type of extraordinary circumstances that require expedited consideration. Absent expedited review, the Commission will be allowed to collect the nation's voter records without first undertaking a Privacy Impact Assessment, an obligation that should certainly attach to the personal information necessary to sustain the country's democratic institutions. Under 28 U.S.C. § 1657(a), this Court must expedite the review of Appellant's appeal.

I. Delay Will Cause Appellant Irreparable Injury

Any delay in resolution of this appeal will cause irreparable injury to EPIC. EPIC is entitled under the E-Government Act of 2002 to access, review, and disseminate a Privacy Impact Assessment prior to the Commission's collection and creation of a new system to collect personal voter data. The District Court held that the failure to produce the Privacy Impact Assessment imposes on EPIC "the very injuries meant to be prevented by the disclosure of information pursuant to the E-Government Act—lack of transparency and the resulting lack of opportunity to hold the federal government to account." Mem. Op. 16–17. *See also Pub. Citizen v. DOJ*, 491 U.S. 440, 447 (1989).

This injury is particular to EPIC because EPIC's mission is to "focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age." Mem. Op. 17. Absent resolution of the claims under the APA, E-Government Act, and Federal Advisory Committee Act, EPIC will be unable to fully "carry out its mission to educate the public regarding privacy issues." Mem. Op. 17. The Commission's failure to produce a Privacy Impact Assessment impairs EPIC's "programmatic activities—educating the public regarding privacy matters— . . . since those activities routinely rely upon access to information from the federal government." Mem. Op. 26.

II. The District Court's Opinion is Subject to Substantial Challenge

EPIC's appeal also presents a substantial challenge to the District Court's decision. The District Court held that the Commission and the Director of White House Information Technology ("DWHIT") were not "agencies," Mem. Op. 27, 32, relying on the "substantial independent authority" test that controls in FOIA cases. *Soucie v. David*, 448 F.2d 1067, 1073 (D.C. Cir. 1971); *see also Citizens for Responsibility & Ethics in Washington v. Office of Admin.*, 566 F.3d 219, 222 (D.C. Cir. 2009); *Armstrong v. Exec. Office of the President*, 90 F.3d 553, 558 (D.C. Cir. 1996) (citing *Meyer v. Bush*, 981 F.2d 1288 (D.C. Cir. 1993).

But the District Court was wrong to allow a FOIA test to govern the outcome of this case: this Circuit's precedents demonstrate that the term "agency" carries distinct meanings under the APA and the FOIA. *Compare Armstrong v. Bush*, 924 F.2d 282, 291 (D.C. Cir. 1991) (applying the APA to the National Security Council ("NSC") as an "agency"), *with Armstrong v. Exec. Office of the President*, 90 F.3d 553, 557–66 (D.C. Cir. 1996) (holding that the NSC is not an "agency" under the FOIA); *see id.* at 566 (The Court's holding under FOIA still left "the question [of] whether the NSC is an 'agency' within the meaning of that term as it is used in the APA. *See* 5 U.S.C. § 551(1) (agency defined as 'each authority of the Government of the United States')."). Nor has this Court ever held that a Presidential Advisory Commission is not subject to the APA or that a Presidential Advisory Commission would not be subject to Section 208 of the E-Government Act of 2002. EPIC's appeal thus represents a substantial challenge requiring the Court's immediate attention.

III. The Public has an Unusual Interest in Prompt Disposition

Finally, non-parties and the public generally also have an unusual and extraordinarily strong interest in a prompt disposition of this case. There are now 512 pages of public comments responding to the Commission's attempt to file personal voter data, the vast majority of which are opposed to the Commission's

proposed collection of state voter records. *See Presidential Advisory Commission on Election Integrity Resources*, The White House.[1]

The vast majority of states have also refused to turn over the voter data the Commission is seeking. *Forty-four States and DC Have Refused to Give Certain Voter Information to Trump Commission,* CNN (July 5, 2017).[2] California Secretary of State Alex Padilla stated on June 29, 2017, that "[t]he President's commission has requested the personal data and the voting history of every American voter–including Californians. As Secretary of State, it is my duty to ensure the integrity of our elections and to protect the voting rights and privacy of our state's voters." Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017).[3] On July 25, 2017, after the district court's ruling, Secretary Padilla reaffirmed that he would not comply with the Commission's request. Press Release, Secretary of State Alex Padilla Reaffirms California Will Not Comply with Kobach Commission

---

[1] https://www.whitehouse.gov/presidential-advisory-commission-election-integrity-resources (last visited July 27, 2017).
[2] http://www.cnn.com/2017/07/03/politics/kris-kobach-letter-voter-fraud-commission-information/index.html.
[3] http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/.

Voter Data Request (July 25, 2017).[4] Nebraska Secretary of State John Gale stated on July 6, 2017 that "I also have a concern about data privacy. I have no clear assurances about the security that this national database will receive. In light of the domestic and foreign attacks in 2016 on state voter registration databases, the commission will need to assure my office of a high level of security." Press Release, Sec. Gale Issues Statement on Request for NE Voter Record Information (July 6, 2017).[5] Arizona Secretary of State Michele Reagan said:

> I share the concerns of many Arizona citizens that the Commission's request implicates serious privacy concerns. [...] Since there is nothing in Executive Order 13799 (nor federal law) that gives the Commission authority to unilaterally acquire and disseminate such sensitive information, the Arizona Secretary of State's Office is not in a position to fulfill your request.
>
> [...]
> Centralizing sensitive voter registration information from every U.S. state is a potential target for nefarious actors who may be intent on further undermining our electoral process. [...] Without any explanation how Arizona's voter information would be safeguarded or what security protocols the Commission has put in place, I cannot in good conscience release Arizonans' sensitive voter data for this hastily organized experiment.

---

[4] http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-reaffirms-california-will-not-comply-kobach-commission-voter-data-request/.

[5] http://www.sos.ne.gov/admin/press_releases/pdf-2017/nr-20170707.pdf.

Letter from Michele Reagan, Arizona Sec. of State, to Kris Kobach, Vice Chair, PACEI (July 3, 2017).[6]

States are debating how to comply with the Commission's request while this appeal is pending. State election officials and their constituents have a strong, vested interest in the prompt resolution of this case so that the personal information of voters is protected.

Considering the need for the utmost expedition in this matter, Appellant proposes the following briefing schedule:

Appellant's Opening Brief	August 18, 2017
Appellees' Brief	September 15, 2017
Appellant's Reply Brief	September 22, 2017

Appellant has contacted Appellees' counsel, and they do not oppose this proposed briefing schedule.

CONCLUSION

For the foregoing reasons, Appellant respectfully requests that consideration of this matter be expedited, that the Court issue an order setting the above briefing schedule, and that the Court direct the Clerk to schedule oral argument on the earliest available date following the completion of briefing.

---

[6] https://assets.documentcloud.org/documents/3884344/Kobach-Response-Letter-DRAFT-1.pdf.

Respectfully Submitted,

/s/ Marc Rotenberg

Marc Rotenberg,
Alan Butler
Caitriona Fitzgerald
Jeramie D. Scott
John Davisson
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140
rotenberg@epic.org

Attorneys for Appellant EPIC

Dated: July 28, 2017

CERTIFICATE OF SERVICE

I, Marc Rotenberg, hereby certify that on July 28, 2017, I electronically filed the foregoing document with the Clerk of the Court for the United States Court of Appeals for the D.C. Circuit by using the CM/ECF system. The following participants in the case who are registered CM/ECF users will be served by the CM/ECF system:

Daniel Tenny
Email: daniel.tenny@usdoj.gov
U.S. Department of Justice
(DOJ) Civil Division, Appellate Staff
Firm: 202-514-2000
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Elizabeth J. Shapiro
Direct: 202-514-5302
Email: elizabeth.shapiro@usdoj.gov
Fax: 202-616-8470
U.S. Department of Justice
(DOJ) Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, DC 20530

Mark B. Stern, Attorney
Email: mark.stern@usdoj.gov
U.S. Department of Justice
(DOJ) Civil Division, Appellate Staff
Firm: 202-514-2000
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

/s/ Marc Rotenberg
MARC ROTENBERG

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6). The motion is composed in a 14-point proportional typeface, Times New Roman, and complies with the word limit of Fed. R. App. P. 27(d)(2)(A) and D.C. Circuit Rule 27(a)(2), because it contains 3,111 words.

/s/ Marc Rotenberg
MARC ROTENBERG

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civ. Action No. 17-1320 (CKK)

REPLY IN SUPPORT OF PLAINTIFF'S AMENDED MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

This week the Presidential Advisory Commission on Election Integrity will meet in Washington, DC. Among the items for consideration is the matter now before this Court. The Commission is seeking to collect the nation's voter records and store that data outside of the privacy laws that routinely attach to an agency of the federal government. Following the initiation of EPIC's lawsuit and widespread opposition by state election officials, the Commission suspended the program, pending the Court's decision. The Court should now enter an order enjoining the Commission from restarting this ill-conceived, poorly executed, and unlawful plan.

Plaintiff EPIC set out multiple arguments in its Amended Motion for a Temporary Restraining Order: the Defendants failed to undertake and publish a Privacy Impact Assessment; the Defendant failed to publish the Privacy Impact Assessment pursuant to the Federal Advisory Committee Act; and, the Defendants' actions violate the constitutional right to information privacy. EPIC established the necessary elements for a TRO: (1) EPIC is likely to succeed on the merits of its claims; (2) EPIC's members will suffer irreparable harm if relief is not granted; and (3) the balance of the equities and public interest favor relief.

18-F-1517//1554

The Defendants' opposition fails to rebut these claims. Moreover, Defendants' standing challenges fails for multiple reasons, including the obvious—the Commission seeks to obtain the voter records of every registered voter in the United States, including EPIC's members. The Commission is seeking not only the personal data of the members of the EPIC Advisory Board, but also the personal data of the vast majority of members of associations across the United States. In this case, it would be difficult to find organization members who do not have standing.

For the reasons set out in Plaintiff's Amended Motion, the responses to the Defendants' Opposition set out in Plaintiff's Reply below, the relevant law, and the record in this matter, Plaintiff's respectfully asks this Court to grant Plaintiff's motion for a preliminary injunction.

ARGUMENT

I. The Defendants' attempts to evade the APA and E-Government act fall flat because they clearly fit within the agency definition

A. The meaning of "Agency" under the APA is not governed by FOIA authorities.

Defendants try, but fail, to elude the APA's broad definition of "agency." Though Defendants spend page after page reciting the supposed parameters of the "agency" test in Part I.B.1 of their Opposition, they once again overlook that the sources cited concern (a) the definition of "agency" as applied to FOIA requests, *e.g.*, *Soucie v. David*, 448 F.2d 1067 (D.C. Cir. 1971); or (b) the applicability of the APA to the President himself, *e.g.*, *Franklin v. Massachusetts*, 505 U.S. 788 (1992). None of these sources support the view that the "sole function" exception applies where, as here, the actions of the EOP and its subcomponents are under APA review.

Defendants wrongly rely on *Dong v. Smithsonian* for the proposition that the "substantial independent authority" test applies to APA claims. 125 F.3d 877 (D.C. Cir. 1997). *Dong* exclusively concerned claims under the Privacy Act, *not* under the APA. *Id.* at 877. Because the Privacy Act itself only applies to government entities that meet FOIA's "agency" definition, 5 U.S.C. § 552a(a)(1) (citing § 552(e)), the *Dong* court was right to rely on the D.C. Circuit's

18-F-1517//1555

FOIA/"substantial independent authority" line of cases. But *Dong* does not govern the meaning of "agency" for the purposes of APA claims, which remains undiluted by *Soucie* and its progeny.

Defendants also lay great stress on the subsequent procedural history of *Alexander v. FBI*, 971 F. Supp. 603 (D.D.C. 1997). But this is an APA case, not a Privacy Act case. The eventual reversal of Judge Lamberth's "interpretation of the Privacy Act"—which, unlike the APA, depends entirely on FOIA's definition of "agency"—has no bearing on Defendants' status as APA agencies. Nor does it weaken the force of Judge Lamberth's overarching observation: that statutes which "provide citizens with better access to government records" and statutes which "provide certain safeguards for an individual against an invasion of personal privacy" serve "very different purposes" and ought to be read accordingly. *Id.* at 606.

B. The Commission and the Director are both agencies under the APA.

The Commission is assuredly an "agency" under the APA, notwithstanding Defendants' claims that it is solely "advisory." Def.'s Opp'n 27. Defendants focus exclusively on what the Commission is *supposed to do* ("study the registration and voting processes used in Federal elections," Exec. Order No. 13,799, 82 Fed. Reg. 22,389) yet ignore the what the Commission is *actually doing* (constructing a massive and unsecure database of nearly 200 million voter records). A government entity may appear "advisory" in form yet be an agency in practice where "the record evidence regarding [the Commission]'s actual functions" proves it to be exercising agency functions. *Citizens for Responsibility & Ethics in Washington (CREW) v. Office of Admin.*, 559 F. Supp. 2d 9, 26 (D.D.C. 2008), aff'd, 566 F.3d 219; *see also* Def.'s Opp'n 29 ("[T]he relevant inquiry is the function exercised . . . ."). That is precisely the scenario here. *See* Pl.'s Am. Mot. 20–21, 28–29.

The Director likewise heads an APA agency. First, Defendants' so-called "controlling authority" on the agency status of the White House Office ("WHO") arises—predictably—out of FOIA and Privacy Act claims. Def.'s Opp'n 31. As noted, these cases are inapplicable to the WHO's status as an APA agency. Second, the Director also describes his agency staff as being

18-F-1517//1556

part of the Office of Administration ("OA"), Herndon Declaration 3, ECF No. 38-1, to which the APA certainly applies. *Pub. Citizen, Inc. v. Lew*, 127 F. Supp. 2d 1, 5, 26 (D.D.C. 2000) (applying the APA to the OA). Finally, it may not "matter" to Defendants that the Director exercises authority over other agencies, Def.'s Opp'n 31, but it does matter to the status of the Director's office as an agency. *Cf. Pub. Citizen v. Carlin*, 2 F. Supp. 2d 1, 9 (D.D.C. 1997), *rev'd on other grounds*, 184 F.3d 900 (D.C. Cir. 1999) ("The EOP's status as an agency is also evidenced by the authority it possesses to impose requirements on all of the EOP components in certain matters."). The Director is thus subject to APA review.

C. The EOP is a discrete agency under the APA and is accountable for the conduct of all subcomponents.

In disavowing any EOP responsibility for the conduct of EOP subcomponents, the Defendants yet again confuse the differing definitions of "agency" under the APA and the FOIA. The "component-by-component analysis" to which the Defendants refer applies only records generated by individual EOP offices, not to the *conduct* of those same offices. Indeed, courts have repeatedly reviewed the EOP's actions under the APA. *Armstrong v. Bush*, 924 F.2d 282, 291 (D.C. Cir. 1991) (applying the APA to both the EOP generally and the National Security Council specifically); *Armstrong v. Exec. Office of the President*, 810 F. Supp. 335, 338 (D.D.C. 1993) (citing *Armstrong*, 924 F.2d at 291–293) ("The Court of Appeals . . . approved of this Court's holding that the APA provides for limited review of the adequacy of the . . . EOP's recordkeeping guidelines and instructions pursuant to the FRA."); *Citizens for Responsibility & Ethics in Washington (CREW) v. Exec. Office of President*, 587 F. Supp. 2d 48, 57–58, 63 (D.D.C. 2008) (holding that the EOP was properly named as a defendant in an APA suit). The Defendants have no answer to these cases, just as they have no answer to the many cases in which the actions of subordinate agencies have been ascribed to parent agencies. Pl. Mot. 23–24.

Moreover, Defendants' position on the applicability of the APA to the EOP is both alarming and absurd. An "absence of judicial review" over the conduct of individual White House offices would lead to intolerable "anomal[ies]." *CREW v. Cheney*, 593 F. Supp. 2d 194, 215

18-F-1517//1557

(D.D.C. 2009). For example, in order to shield his administration's actions from scrutiny, a President could simply establish a new White House office and define its powers as being coextensive with "any government agency or employee of the United States." *CREW*, 593 F. Supp. 2d at 215 (*Armstrong v. Exec. Office of the President, Office of Admin.*, 1 F.3d 1274, 1292 (D.C. Cir. 1993)). "If this definition were implemented without the possibility of judicial review," it would "functionally render the [APA] a nullity." *Id.* The Court should reject that path.

Because it is an agency responsible for the action of its constituent offices, the EOP should be enjoined from collecting personal voter data.

D. The E-Government Act applies to defendants, just as the Paperwork Reduction Act does.

Though Defendants labor to exempt themselves from the definition of "agency" under the E-Government Act of 2002, Pub. L. 107-347, 115 Stat. 2899, Title II § 208 (codified at 44 U.S.C. § 3501 note), they cannot escape the plain text and history of the provision.

First, although the FOIA's definition of agency and the E-Government Act's definition of "agency" are quite similar, they are not perfectly coextensive. *Compare* § 5 U.S.C. § 552(f)(1), *with* 44 U.S.C. § 3502(1). Crucially, the FOIA's definition "agency" identifies no government entities that are expressly excluded from the FOIA, relying instead on the APA's list of exclusions. *See* 5 U.S.C. §§ (1)(A)–(H). To the extent that any government entities are *specifically* excused from FOIA obligations, they are excused solely by legislative history. *See* H.R. Rep. No. 93-1380, at 232 (1974) (Conf. Rep.); *see also Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 156 (1980).

By contrast, the E-Government Act's definition of "agency" *expressly identifies* the government entities that are excluded from the Act. § 3502(1)(A)–(D). Had Congress intended for subcomponents of the Executive Office of the President to fall outside of § 3502(1), Congress would have said so when it drafted the provision in 1980. Paperwork Reduction Act of 1980, Pub. L. No. 96-511, § 2, 94 Stat. 2812, 2813 (codified as amended at § 3502) ("PRA"). But Congress did not, and the legislative history of the Act reveals no hidden intent to make such exclusions.

18-F-1517//1558

The Court should decline Defendants' invitation to disregard the clear language of § 3502(1) and refuse to read into the provision a nonexistent exception for EOP subcomponents. *Milner v. Dep't of Navy*, 562 U.S. 562, 572 (courts should not "allow[] ambiguous legislative history to muddy clear statutory language.").

Moreover, both case law and the OMB confirm that defendants are "agenc[ies]" for the purposes of the E-Government Act. The term "agency" under the E-Government Act means the same thing as it does under the PRA. And the White House Office ("WHO"), the Director of White House Information Technology ("DWHIT"), and the Commission—like other subcomponents of the EOP—are agencies subject to the PRA. *See Pub. Citizen*, 127 F. Supp. 2d at 5, 26 (ordering the OA, the U.S. Trade Representative, and the OMB to comply with "their obligations under . . . the PRA"); *see also* Herndon Decl. 1, 6, ECF No. 38-1 (interchangeably describing the Director of White House Information Technology as being part of the White House Office and the Office of Administration). The Defendants are therefore agencies subject to the E-Government Act. *See Lorillard v. Pons*, 434 U.S. 575, 581 (1978) ("Congress normally can be presumed to have had knowledge of the interpretation given to the incorporated law, at least insofar as it affects the new statute"). Further, these agencies' compliance with the E-Government Act is reviewable under the APA. *See Pub. Citizen*, 127 F. Supp. 2d at 5, 26.

The OMB, which is charged with primary authority to implement the PRA, 44 U.S.C. § 3504, has long understood the EOP and its subcomponents to be agencies under the Act. The OMB has for many years issued control numbers under the PRA to the EOP, the WHO, and the Council on Environmental Quality (a further subcomponent of the EOP). *Search of Information Collection Review*, Office of Info. & Reg. Affairs.[1] Moreover, from the moment the PRA was enacted, the OMB understood the OA to be subject to the PRA's requirements. 127 Cong. Rec. S11,159, 11,159–60 (daily ed. Oct. 6, 1981) (listing the OA as an "agency" subject to the PRA). Defendants are thus agencies subject to the E-Government Act.

[1] https://www.reginfo.gov/public/do/PRASearch (last visited July 17, 2017).

18-F-1517//1559

E. The General Services Administration cannot duck its independent obligations as an Agency.

Defendants, apparently eager to escape APA review, present a deeply confused version of EPIC's arguments concerning the General Services Administration ("GSA"). Def.'s Opp'n 33. The point is simple: the GSA is legally required to store any data that the Commission collects, yet the GSA failed to do so. The Charter states that the GSA is the "*Agency Responsible for Providing Support.*" Charter § 6 (emphasis added). This is entirely consistent with the plain text of the Executive Order, which assigns to the GSA—and no other entity—responsibility to provide "facilities," "equipment," and "other support services" as "may be necessary to carry out [the Commission's] mission." Exec. Order No. 13,799, 82 Fed. Reg. 22,389. The GSA, which is indisputably an agency, was also required to conduct and publish a PIA before such collection. The agency's actions—and inaction—are thus plainly unlawful under the Executive Order, the APA, and the E-Government Act and should be enjoined as such.

II. The cases cited by Defendants support EPIC's informational privacy claim.

In arguing against the claim to information privacy, the Defendants places considerable weight on *Doe v. City* of N.Y., 15 F.3d 264, 268 (2d Cir. 1994) (citing *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 493-96 (1975). The Defendants find this statement in that opinion: "there is no question that an individual cannot expect to have a constitutionally protected privacy interest in matters of public record." Opp at 34.

That was dicta, noting a point made by the defendants in that case. In *Doe*, the Second Circuit actually held "There is, therefore a recognized constitutional right to privacy in personal information." *Id.* at 267. The Second Circuit found that "Individuals who are affected with the HIV virus clearly possess a constitutional right to privacy regarding their condition." Id. The Second Circuit concluded:

> In sum, we hold that Doe has a right to privacy (or confidentiality) in his HIV status, because his personal medical condition is a matter that he is normally entitled to keep private. We also hold that Doe's HIV status did not, as a matter of law, automatically become a public record when he filed his claim with the Commission and entered into the Conciliation Agreement.

18-F-1517//1560

Id. at 269.

The argument that the Defendants make here is similar to the one made by New York Commission in *Doe*: by virtue of providing information to a state agency, the individual has waived whatever constitutional privacy claims she may have. The Second Circuit rejected that conclusion. It recognized a right to information privacy.

Similarly, in *Lewis v. Delarosa*, No. C 15-2689 NC (PR), 2015 WL 5935311, at *1 (N.D. Cal. Oct. 13, 2015), cited by the Commission, Def.'s Opp. 34, the magistrate judge court acknowledged a constitutional right to privacy recognized, noting that

> The Ninth Circuit has recognized a "constitutionally protected interest in avoiding disclosure of personal matters including medical information," but that interest is conditional, not absolute. *Seaton v. Mayberg*, 610 F.3d 530, 538 (9th Cir. 2010); see *In re Crawford*, 194 F.3d 954, 958-59 (9th Cir. 1999) (recognizing informational privacy as a constitutionally protected interest but one that is not absolute); *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1269 (9th Cir. 1998) (stating that "[t]he constitutionally protected privacy interest in avoiding disclosure of personal matters clearly encompasses medical information and its confidentiality," and [*9] holding that blood and urine tests administered to collect medical information implicated such a right under the Fifth or Fourteenth Amendments). In comparison to *Seaton* and *Norman-Bloodsaw*, Plaintiff's allegation that his right to informational privacy was violated when his non-private identification information was published on the internet is not included in even the outer confines of a federal right to informational privacy.

Lewis, 2015 WL 5935311, at *3.

Regarding *NASA v. Nelson*, 562 U.S. 134, 138 (2011), EPIC's Amended Motion provides a more complete analysis of the reasoning in in that case than the Defendants provide. See Amd. Mot 30-34. Specifically, EPIC points to Justice Alito's holding for the Court which relied on the "the protection provided by the Privacy Act's nondisclosure requirement" and the fact that the information sought was "reasonable." NASA, 562, U.S. at 159. Amd. Mot at 32. The Defendants' have specifically disavowed any privacy obligations in the collection of the state voter record information and the request is widely viewed by state election officials as "unreasonable." *See, e.g.*, Ex. 20.

18-F-1517//1561

Even the Commission's analysis of D.C. Circuit law is misleading. In *AFGE*, the Court found "sufficiently weighty interests" to justify the collection of certain personal information in employee surveys. *Am Fed. Of Gov't Emps., AFL-CIO v. Dep't of House & Urban Dev.*, 118 F.3d 786, 791 (D.C Cir. 1997) ("AFGE"). But the D.C. Circuit also observed:

> [S]everal of our sister circuits have concluded based on *Whalen* and *Nixon* that there is a constitutional right to privacy in the nondisclosure of personal information. *See United States v. Westinghouse Electric Corp.*, 638 F.2d 570, 577-580 (3d Cir. 1980) (holding that there is a constitutional right to privacy of medical records kept by an employer, but that the government's interest in protecting the safety of employees was sufficient to permit their examination); *Plante v. Gonzalez*, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978), cert. denied, 439 U.S. 1129 (1979) (identifying a "right to confidentiality" and holding that balancing is necessary to weigh intrusions); *Barry v. City of New York*, 712 F.2d 1554, 1559 (2d Cir. 1983), *cert. denied*, 464 U.S. 1017 (1983) (applying an intermediate standard of review to uphold a financial disclosure requirement). *See also, Hawaii Psychiatric Soc'y Dist. Branch v. Ariyoshi*, 481 F. Supp. 1028, 1043 (D. Hawaii 1979) (holding that disclosure of psychiatric records implicates the constitutional right to confidentiality); *McKenna v. Fargo*, 451 F. Supp. 1355, 1381 (D.N.J. 1978) ("The analysis in Whalen ... compels the conclusion that the defendant . . . must justify the burden imposed on the constitutional right of privacy by the required psychological evaluations.").

118 F.3d at 792. The D.C. Circuit in *AFGE* concluded:

> Having noted that numerous uncertainties attend this issue, we decline to enter the fray by concluding that there is no such constitutional right because in this case that conclusion is unnecessary. Even assuming the right exists, the government has not violated it on the facts of this case. Whatever the precise contours of the supposed right, both agencies have presented sufficiently weighty interests in obtaining the information sought by the questionnaires to justify the intrusions into their employees' privacy.

AFGE v. HUD, 326 U.S. App. D.C. 185, 118 F.3d 786, 793 (1997).

In the matter before this Court, the Defendants have presented no such "sufficiently weighty interests." In fact, the Commission's attempt to obtain state voter records is seen by election officials as intrusive and unnecessary.

The Defendants' tautological use of the phrase "publicly available" obscures the Commission's intent and does not mitigate the privacy risks. The Commission is explicitly seeking detailed personal data maintained by the states and protected by state law. *See* Ex. 2.

18-F-1517//1562

Invoking the phrase "publicly available" further obscures the procedures that any requester seeking state voter records, such as the designation of files, the payment of fees, the completion of forms, and the provision of a secure transmission method would otherwise be required to follow. *See* Pl.'s Reply 16–17, ECF No. 13.

The Defendants go out of their way to discuss *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), a case that is favorable to EPIC but which Plaintiff simply chose to omit from the earlier briefing. Notably, *in Reporters Committee* the Court considered whether rap sheets stored in state record systems acquired a privacy interest when they were centralized and stored in a federal records system. Assessing the scope of exemption 7(c) in the Freedom of Information Act, the Court upheld the privacy interest. Justice Stevens writing for the Court concluded:

> Accordingly, we hold as a categorical matter that a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no "official information" about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is "unwarranted."

Reporters Committee, 489 U.S. at 780.

Reporter's Committee is generally viewed as a case concerning statutory construction. But to the extent that it bears on EPIC's constitutional claims, which Defendants apparently believe it does, it would weigh in favor of the relief EPIC seeks.

III. The Defendants' irreparable harm arguments ignore the mounting evidence that voters will be harmed absent an injunction.

The Defendants' contention that no irreparable harm will occur is directly contradicted by the Commission's own statements and actions, by the actions of the Arkansas Secretary of State, and by this Court's prior decisions recognizing the inherent harm caused by improper disclosure of confidential information. But the Defendants cannot escape the fact that the Commission is seeking to collect sensitive, personal information about every registered voter in America. *See* First Kobach Decl., Ex. 3. Why would the Commission demand disclosure of the SSNs, dates of birth, felony convictions, and political affiliations of voters if it did not believe that it would in

18-F-1517//1563

fact receive that data? The Defendants failure to address this obvious question speaks volumes. Indeed, the Defendants argument works much better in reverse, *see* Def's Opp'n 37, n.9, if the Commission does not intend to collect sensitive and confidential voter data, then they never should have requested it and they would not suffer any setback if this Court enjoins such collection. There is simply no reason to permit the Defendants to collect any voter data during the pendency of this case.

The Commission's attempts to collect personal voter data by improperly inducing states to release the records outlined in the Kobach letter are well established in the record. The Commission has clearly and repeatedly expressed its intention to collect the "last four digits of social security numbers," "political party" information, and "dates of birth" in addition to other personal voter data. First Kobach Decl. ¶ 4; Pl.'s Ex. 3. Where states have expressed resistance, the Commission has used that as an excuse to question their motives in statements to the public. *See* FOX & Friends (@foxandfriends), Twitter (Jul. 6, 2017, 3:23 am) (".@VPPressSec: For the 14 states not complying with the voter commission, what are they trying to hide? Or is this just pure partisanship?").[2] The Defendants cannot simultaneously seek to coerce states into providing sensitive voter data and then claim that it would be the states fault if the data is improperly disclosed. Def.'s Opp'n 37, n.9. The Commission has clearly expressed its intent to collect this data, and the Court has the authority to enjoin such collection where it would cause irreparable harm.

The Defendants attempted reliance on the "presumption of regularity" also fails here where we have already seen one state, Arkansas, attempt to transfer data to the Commission through an insecure system in violation of both state and federal law. *See* Ark. Code Ann. § 25-19-105(a)(1)(A) ("Except as otherwise specifically provided by this section or by laws specifically enacted to provide otherwise, all public records shall be open to inspection and copying by any *citizen* of the State of Arkansas during the regular business hours of the custodian

[2] https://twitter.com/foxandfriends/status/882907901420896256.

18-F-1517//1564

of the records."). The Defendants have not provided any evidence that the Commission is a "citizen" of Arkansas or could otherwise lawfully access any state voter data. Other states have similarly indicated that they will provide data to the Commission in violation of state law. For example, New Hampshire Secretary of State has said that he will share voters' names, addresses, party affiliation and voting history dating back to 2006. This violates state law, which allows for the inspection but not the transfer of voter registration data:

> Any person may view the data that would be available on the public checklist, as corrected by the supervisors of the checklist, on the statewide centralized voter registration database maintained by the secretary of state at the state records and archives center during normal business hours, but the person viewing data at the state records and archives center may not print, duplicate, transmit, or alter the data. N.H. Rev. Stat. § 654:31(III)

New Hampshire law only permits the transfer of voter registration lists to a "political party" or "political committee." N.H. Rev. Stat. § 654:31(IV).

The Commission's recent actions also validate EPIC's claims that any personal data collected can be improperly disclosed. Additionally, the Defendants have already revealed personally identifiable information by publishing the names, email addresses, and other sensitive information of members of the public who have contacted the Commission with questions and feedback. *Presidential Advisory Commission on Election Integrity Resources*, The White House (2017).[3] Many of these messages were sent prior to the Commission's July 5 publication of a notice that it "might" publish identifying information from commenters. The Presidential Commission on Election Integrity (PCEI); Upcoming Public Advisory Meeting, 82 Fed. Reg. 31,063 (July 5, 2017).

IV. The Defendants fail to rebut the evidence EPIC has provided, which establishes informational and organizational injuries as well as associational standing as required under Article III.

The Defendants' standing arguments ignore the well-pled allegations in EPIC's Second Amended Complaint as well as the supplementary evidence provided in this case, including

[3] https://www.whitehouse.gov/presidential-advisory-commission-election-integrity-resources.

18-F-1517//1565

declarations by EPIC's Executive Director and the individual declarations of Members of the EPIC Advisory Board. Rather than respond to these exhibits that are in the record, the Defendants misconstrues the D.C. Circuit's recent decision in *Friends of Animals* and misrepresent EPIC's structure, purpose, and relationship to its members. But the Court need not follow the Defendants down these rabbit holes. The record clearly shows that EPIC has established informational standing, organizational standing, and associational standing on behalf of its members.

A. EPIC has established informational standing.

The Court should reject the Defendants' proposed interpretation of informational injury under Article III because it would produce an absurd result. The Defendants' argument is based on the flawed premise that no plaintiff can challenge an agency's failure to produce a record as required by law when the agency refuses to create it. Def.'s Opp'n 15. Such a sweeping argument would be contrary to the Supreme Court's holding in *Public Citizen* and is not supported by the D.C. Circuit's recent decision in *Friends of Animals*. Not only is the Defendants' view contrary to precedent, it would undermine the purpose of the E-Government Act, which is to ensure the protection of personal data prior to its acquisition, and produce illogical results.

EPIC has properly asserted standing based on the well-pled allegation that Defendants' failure to release a Privacy Impact Assessment for the proposed collection of personal voter data would cause an informational injury to EPIC and directly impact EPIC's organizational mission and public education functions. Second Am. Compl. ¶¶ 5, 67–76. An informational injury occurs when a plaintiff is denied information due to it under statute. *FEC v. Akins*, 524 U.S. 11, 21 (1998). The D.C. Circuit explained in *Friends of Animals v. Jewel* , 828 F.3d 989, 992, (D.C. Cir. 2016) that:

> A plaintiff suffers sufficiently concrete and particularized informational injury where the plaintiff alleges that: (1) it has been deprived of information that, on its interpretation, a statute requires the government or a third party to disclose to it, and (2) it suffers, by being denied access to that information, the type of harm Congress sought to prevent by requiring disclosure.

18-F-1517//1566

Id. "Anyone whose request for specific information has been denied has standing to bring an action; the requester's circumstances—why he wants the information, what he plans to do with it, what harm he suffered from the failure to disclose—are irrelevant to his standing." *Zivotofsky v. Sec'y of State*, 444 F.3d 614, 617 (D.C. Cir. 2006). Further, denial of "timely access" to information constitutes an "informational injury" to which the government can "make no serious challenge to the injury and causation elements . . . of standing." *Byrd v. EPA*, 174 F.3d 239, 243 (D.C. Cir. 1999).

The Defendants' attempt, in a footnote, to distinguish the D.C. Circuit's decision in *PETA v. USDA*, 797 F.3d 1087 (D.C. Cir. 2015), reveals the incoherence of their proposed informational injury test. Def.'s Opp'n 15, n.1. Just like the plaintiffs in *PETA*, EPIC has established that the Defendants' failure to release a privacy impact assessment "directly conflicted with its mission of public education" and investigations into government privacy practices. *PETA*, 797 F.3d at 1095. The Defendant concedes that the court in *PETA* found there was Article III standing even without an express statutory guarantee to "preexisting information," Def's Opp'n 15, n.1, which means that EPIC has an even stronger standing claim that PETA. There can be no question that the organizational and informational injury in this case is "self-evident," Def's Opp'n 8, where EPIC's core mission is to "focus public attention on emerging privacy and civil liberties issues" by conducting "oversight and analysis of government activities," Second Am. Compl. ¶ 5. By refusing to release a Privacy Impact Assessment as required by law, the Defendants have increased the burden on EPIC to conduct its "oversight and analysis" in a more costly and resource-intensive way that would not otherwise be necessary. See Decl. of Eleni Kyriakides.

The cases cited in the opposition are easily distinguishable and do not support the improperly narrow scope of informational injury that the Defendants assert here. Both *Friends of Animals v. Jewell*, 828 F.3d 989, 992, (D.C. Cir. 2016), and *Am. Farm Bureau v. EPA*, 121 F. Supp. 2d 84, 94 (D.D.C. 2000), involved enforcement of "statutory deadline provision[s]" rather than disclosure provisions. The court in *Friends of Animals* went out of its way to draw this distinction. 828 F.3d at 993 ("Friends of Animals's complaint seeks to have the court order

18-F-1517//1567

compliance with section 4(b)(3)(B)'s deadline requirement, not its disclosure requirement."). Unlike the Endangered Species Act at issue in *Friends of Animals*, the E-Government Act provision at issue in this case requires the creation and disclosure of a Privacy Impact Assessment by the agency *prior to* initiating the collection of personal information. E-Government Act § 208(b) ("An agency shall take actions described under paragraph (B) *before* . . . initiating a new collection of information . . . ."). Where, as here, Congress has required the creation of a document prior to a specifically defined agency action, and the agency has taken that action, a plaintiff in EPIC's position can assert an informational injury for failure to disclose the document. *See* Def.'s Opp'n 16 (citing *Friends of Animals* test showing that the precondition for disclosure had not been met in that case).

Indeed, EPIC's asserted informational injury is consistent with the Supreme Court's holding in *Public Citizen* that failure to produce records from an advisory committee gives rise to an informational injury, even if those records do not yet exist. *Pub. Citizen v. DOJ*, 491 U.S. 440, 447 (1989). In *Public Citizen*, the plaintiff-appellants sought to compel a committee to disclose, *inter alia*, (1) its charter and (2) advance notices of future committee meetings. *Id.* at 447–48. None of these putative government records existed at the time the plaintiff sought them because the committee disputed that it had any statutory obligation to record or file them. *Id.* Nonetheless, the Court held that the plaintiffs had Article III standing to demand their disclosure:

> Appellee does not, and cannot, dispute that appellants are attempting to compel [the defendants] to comply with [the Federal Advisory Committee Act]'s charter and notice requirements . . . . As when an agency denies requests for information under the Freedom of Information Act, refusal to permit appellants to scrutinize the ABA Committee's activities to the extent FACA allows constitutes a sufficiently distinct injury to provide standing to sue.

Id. at 449. EPIC is in the same position as Public Citizen: seeking public disclosure of an advisory committee document which the Commission must by law record (here, a Privacy Impact Assessment). That the Commission has failed to record such a document is no bar to EPIC's information-based standing, just as it was no bar in *Public Citizen*. *Id.* at 449.

18-F-1517//1568

Notably, the court in *Public Citizen* found standing despite the Defendants' contention that a favorable decision "would likely [not] redress the [plaintiffs'] alleged harm because the . . . records they wish to review would probably be" unavailable to them. *Id.* at 449. Here, by contrast, a favorable decision would redress EPIC's informational injury by forcing the Commission to comply with its recording and disclosure obligations. Second Am. Compl. ¶¶ 67–76, p. 15 ¶ D. Even if the Commission seeks to duck its obligation to record a PIA—thereby denying EPIC the ability to review such a document—*Public Citizen* is explicit that EPIC's "potential gains [would] undoubtedly [be] sufficient to give [it] standing" to demand disclosure. *Id.* at 451.

EPIC also easily satisfies the test in *Friends of Animals* for informational injury standing. First, EPIC has alleged that it was "deprived of information that . . . a statute requires the government . . . to disclose to it," *Friends of Animals*, 828 F.3d at 992. EPIC—by itself and through its members—was denied access to Commission information under the E-Government Act of 2002, 44 U.S.C. § 3501 note, and the FACA, U.S.C. app. 2 § 10(b). Second Am. Compl. ¶¶ 5, 67–76; *see* 5 U.S.C. § 706(1); *Am. Friends Serv. Comm. v. Webster*, 720 F.2d 29, 57 (D.C. Cir. 1983) (finding plaintiffs in an APA suit "[met] the 'zone of interests' test for standing" because the agency's violations of a records statute obstructed the "public's expected access to records"). Second, the harm EPIC has suffered is one that "Congress sought to prevent": a denial of "citizen access to Government information." Pub. L. 107–347, 116 Stat 2899, 2899; *see also* Pub. L. 92–463, 86 Stat. 770, 770 ("[T]he public should be kept informed with respect to the . . . activities . . . of advisory committees[.]"). EPIC has thus alleged a valid informational injury. *See PETA*, 797 F.3d at 1095 (holding "denial of access to . . . information" was a "cognizable injury sufficient to support standing" in APA suit); *Am. Historical Ass'n v. NARA*, 516 F. Supp. 2d 90, 107 (D.D.C. 2007) ("Plaintiffs have standing to pursue their claim that the delay [in obtaining access to records] . . . violates the APA.").

18-F-1517//1569

B. EPIC has established organizational standing.

The Defendants' opposition to EPIC's organizational standing claims rests on a fundamental misreading of EPIC's complaint, EPIC's declaration, and EPIC's website. A brief review of these materials in the record, and an understanding of EPIC's core mission, makes clear that EPIC's organizational standing claim is "self-evident" and does not require special supplemental pleadings as the Defendants concede. Def.'s Opp'n 8. However, EPIC is more than happy to supplement the record in this case to further support its organizational standing claim. EPIC has already suffered a "concrete and demonstrable injury to [its] activities – with a consequent drain on [its] resources" that meets the *NAHB v. EPA* test, 667 F.3d 6, 11 (D.C. Cir. 2011). Specifically, EPIC has diverted resources to investigating the Commission's collection of all Americans' voter records, a program whose secrecy has directly impaired EPIC's mission. *See* Kyriakides Decl..

EPIC's core mission and activities—namely, "public education" and the "protect[ion of] privacy, free expression, [and] democratic values . . . ," are unquestionably harmed by the Defendants behavior in this case. *See About EPIC*, EPIC. org (2015).[4] EPIC's mission includes, in particular, educating the public about the government's record on voter privacy and promoting safeguards for personal voter data. *See, e.g.*, *Voting Privacy*, EPIC.org (2017);[5] EPIC, Comment Letter on U.S. Election Assistance Commission Proposed Information Collection Activity (Feb. 25, 2005).[6] The Commission's failure to carry out a Privacy Impact Assessment and disregard for the informational privacy rights of U.S. voters have thus injured EPIC by making EPIC's "activities more difficult" and creating a "direct conflict between the [Commission's] conduct and [EPIC's] mission." *Nat'l Treasury Empls. Union v. United States*, 101 F.3d 1423, 1430 (D.C. Cir. 1996).

The cases cited by the Defendants in opposition are entirely distinguishable. Def.'s Opp'n 9–11. EPIC's organizational injuries in this case bear no relationship to the "pure issue-advocacy"

[4] https://epic.org/about.
[5] https://epic.org/privacy/voting/.
[6] https://epic.org/privacy/voting/register/eac_comments_022505.html.

18-F-1517//1570

claims dismissed by prior courts. *See Nat'l Consumer League v. Gen. Mills, Inc.*, 680 F. Supp. 2d 132, 136 (D.D.C. 2010) (dismissing issue advocacy claims where the challenged agency action provided a means to carry out the organizational mission); *Ctr. for Law & Educ. V. Dep't of Educ.*, 396 F.3d 1152, 1162 (D.C. Cir. 2005) (rejecting a claim based on "pure issue-advocacy" activities).

The decision in EPIC's prior challenge to changes in specific Department of Education regulations is similarly irrelevant to the issue in this case. That case did not involve agency action that *inhibited* EPIC's ability to inform the public about emerging privacy issues or to conduct oversight of government activities. *EPIC v. Dep't of Educ.*, 48 F. Supp. 3d 1, 23 (D.D.C. 2014) (finding that the challenge to the regulations was part of EPIC's advocacy mission). Unlike the "advocacy" activities at issue in these earlier cases, Defendants' refusal to disclose information and the resulting burden to EPIC's public education and oversight mission in this case clearly creates a "concrete and demonstrable" injury similar to what the D.C. Circuit recently recognized in *PETA*.

Like the plaintiffs in *PETA v. USDA*, 797 F.3d 1087 (D.C. Cir. 2015), EPIC has had to expend organizational resources "in response to, and to counteract, the effects of defendants' alleged [unlawful conduct]." *Id.* at 1097. Simply to preserve the status quo—wherein the federal government was *not* illegally aggregating the personal voter data of nearly 200 million Americans, and wherein EPIC was better able to educate the public about the privacy safeguards in place on all major federal databases of personal information—EPIC has been forced to expand its long-running work on voter privacy. For example, EPIC has had (1) to draft and seek expert sign-ons for a letter urging state election officials to "protect the rights of the voters . . . and to oppose the request from the PACEI," Letter from EPIC et al. to Nat'l Ass'n of State Sec'ys (July 3, 2017);[7] (2) to seek records from the Commission concerning its collection of voter data, *see* Kyriakides Decl., (3) to develop a webpage with extensive information on the Commission's

[7] https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf.

activities. *Voter Privacy and the PACEI*, EPIC.org (2017);[8] and (4) respond to numerous requests from state election officials, citizen organizations, and news organizations concerned about the impact of the Commission's request for voter data on personal privacy.

The Defendants actions have had a direct impact on EPIC's mission and work and imposed a strain on EPIC's resources to fulfill its public education and oversight mission. This is the type of "concrete and demonstrable injury to" EPIC's "organizational activities" that courts have long deemed sufficient for standing. *Havens*, 455 U.S. at 379; *see also PETA*, 797 F.3d 1087 (holding that a non-profit animal protection organization had standing under *Havens* to challenge the USDA's failure to promulgate bird-specific animal welfare regulations); *Abigail All. for Better Access to Developmental Drugs v. Eschenbach*, 469 F.3d 129 (D.C. Cir. 2006) (finding that a health advocacy organization had organizational standing under *Havens* to challenge an FDA regulation). EPIC has established organizational standing under Article III.

C. EPIC has established associational standing.

The Defendants' attempt to distinguish EPIC from other membership organizations fails as well, Def's Opp'n 12–13, and the "formal" relationship between EPIC and its members is a matter of public record that cannot be seriously disputed, *see* EPIC, *Advisory Board* (2017).[9] The programmatic guidance and financial support that EPIC's members provide is similarly a matter of public record. *See* EPIC, *2017 EPIC Champion of Freedom Awards Dinner* (2017) (listing EPIC's Advisory Board members as the primary supporters of EPIC's annual awards dinner);[10] Br. of Amici Curiae EPIC, Thirty Technical Experts and Legal Scholars, and Five Privacy and Civil Liberties Organizations in Support of Petitioner, *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017) (No. 15-1194).[11] There is also no doubt that EPIC's members, most of whom are registered voters in the United States, will suffer a concrete and particularized injury when the

[8] https://epic.org/privacy/voting/pacei/.
[9] https://epic.org/epic/advisory_board.html.
[10] https://epic.org/june5/.
[11] https://epic.org/amicus/packingham/packingham-amicus-EPIC.pdf.

18-F-1517//1572

Defendants improperly collect their sensitive personal information.[12] Based on the record in this case, EPIC easily satisfies both the traditional membership test and the "functional" three-part test under *Washington Legal Foundation v. Leavitt*, 477 F. Supp. 2d 202, 208 (D.D.C. 2007).

The Defendant cannot seriously contend that EPIC "does not appear to serve a specialized segment of the community." Def.'s Opp'n 13. EPIC is a privacy organization, whose core constituents are "members" of the "distinguished advisory board, with expertise in law, technology, and public policy." EPIC, *About EPIC* (2017).[13] If EPIC does not serve a "specialized segment of the community," then it is not clear what membership organization does. The fact that EPIC does not leave membership open to the broader public, Def.'s Opp'n 12, only further supports its specialized nature.

Furthermore, members of EPIC's Advisory Board qualify as "members" for the purposes of Article III standing because they occupy the same roles and fulfill the functions as the "members" that have repeatedly supported associational standing in this Circuit. *See, e.g.*, *Sierra Club v. Fed. Energy Regulatory Comm'n*, 827 F.3d 59, 65 (D.C. Cir. 2016); *Ctr. for Biological Diversity v. EPA*, No. 14-1036, 2017 WL 2818634, at *6 (D.C. Cir. June 30, 2017). All of the above-named declarants are formally identified as "members" of the organization. Declaration of Marc Rotenberg ¶ ¶ 8–12, Ex. 38. More importantly, these EPIC members play a functional role in "selecting [EPIC's] leadership, guiding its activities, [and] financing those activities." *Fund Democracy, LLC v. SEC*, 278 F.3d 21, 26 (D.C. Cir. 2002); *see also Hunt v. Washington State*

---

[12] EPIC has established associational standing on behalf of numerous EPIC members whose privacy is threatened by the Commission's unlawful collection of personal voter data. Voter Declaration of Kimberly Bryant, Ex. 1; Voter Declaration of Julie E. Cohen, Ex. 2; Voter Declaration of William T. Coleman III, Ex. 3; Declaration of Harry R. Lewis, Ex. 4; Voter Declaration of Pablo Garcia Molina, Ex. 5; Voter Declaration of Peter G. Neumman, Ex. 6; Voter Declaration of Bruce Schneier, Ex. 7; Voter Declaration of James Waldo, Ex. 8; Voter Declaration of Shoshana Zuboff, Ex. 9. As each of the above-named EPIC members has attested: "The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm." *See* Voter Declarations, Exs. 1–9.

[13] https://epic.org/epic/about.html.

18-F-1517//1573

Apple Adver. Comm'n, 432 U.S. 333 (1977) (holding that the Washington State Apple Advertising Commission had standing to file suit on behalf of apple growers and dealers because it was "the "functional equivalent of a traditional membership organization."); *Friends of the Earth, Inc. v. Chevron Chem. Co.*, 129 F.3d 826 (5th Cir. 1997) (holding that nonprofit environmental protection corporation with no legal members under the corporate laws of the District of Columbia had standing to file suit on behalf of individuals who voluntarily identified as "members" and played a role in funding and selecting the corporation's leadership). Here, the members of the EPIC Advisory Board commit to the mission of the organization, participate in the work of the organization, and provide financial support to the organization. Rotenberg Decl. ¶ ¶ 8–12.

Defendants have placed considerable weight on the term "advisory" in the titles of EPIC's members, but this distinction is meaningless for Article III standing purposes. Def. Surreply 2–3. First, emphasis on this term ignores the direct and material role that advisory board members play in EPIC's operation, as described above. Moreover, the word "advisory" is not a magic talisman that strips an organization of associational standing where the organization would otherwise enjoy it. *See, e.g.*, *Resident Advisory Bd. v. Rizzo*, 425 F. Supp. 987, 1010 (E.D. Pa. 1976) ("Resident *Advisory Board*" enjoyed associational standing to sue on behalf of members (emphasis added)), *modified on other grounds*, 564 F.2d 126 (3d Cir. 1977); *Oregon Advocacy Ctr. v. Mink*, 322 F.3d 1101, 1110–1112 (9th Cir. 2003) (holding that beneficiaries of organization's work were the "the functional equivalent of members for purposes of associational standing" where they "composed more than 60 percent of the *advisory council*" of that organization (emphasis added)); *State of Connecticut Office of Prot. & Advocacy for Persons with Disabilities v. Connecticut*, 706 F. Supp. 2d 266, 284 (D. Conn. 2010) (holding that state office enjoyed associational standing to sue on behalf of the beneficiaries of its work given that those beneficiaries comprised least 60 percent of the "*Advisory Council*"; given the "specified functions of the *Advisory Council*"; and given "the influence of the *Advisory Council*" over the office's work (emphasis added)).

18-F-1517//1574

The Defendants' argument that EPIC cannot assert an injury on behalf of its members because of certain state responses to the Commission's unlawful demand, Def's Opp'n 13–14, is not supported by the record and is directly contradicted by the Defendants' own submissions. In support of its argument, the Commission referred to EPIC's webpage on the Commission, which provides the public with information about the June 28, 2017 letter and subsequent developments. Def. Surreply 2. EPIC's webpage, which was not authored and has not been reviewed by any state official, lists states that have expressed *opposition* to the Commission's unlawful demand for personal voter data. Def. Surreply, Ex. 1 at 5. The Commission uses the term "reject," but cites no evidence that supports the conclusion that the Commission will not follow through on its plan to collect comprehensive personal voter data—as evidenced by the letters sent on June 28, 2017—to all 50 states and the District of Columbia. *See* Kobach Decl. ¶¶ 4–6. In fact, the Vice Chair has indicated that it is his "belief that there are inaccuracies in those media reports with respect to various states." Kobach Decl. ¶ 6.

Second, EPIC's members will necessarily suffer injuries in fact if the Commission is allowed to carry out its plans. As EPIC has explained, the unlawful collection and aggregation of state voter data, standing alone, constitutes an injury in fact. Pl. Mem. 17; *Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 76 (D.D.C. 2009) (holding that the wrongful disclosure of confidential information is a form of injury); *Hosp. Staffing Sols., LLC v. Reyes*, 736 F. Supp. 2d 192, 200 (D.D.C. 2010) ("This Court has recognized that the disclosure of confidential information can constitute an irreparable harm because such information, once disclosed, loses its confidential nature."). Though it is unlawful for the Commission to obtain voter data without (1) conducting a PIA and (2) adhering to constitutional strictures on the collection of personal information, that is *precisely* what the Commission promises to do—and by a date certain (July 14). The injuries to EPIC's members are thus "certainly impending." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 133 (2013). The Government cannot confidently assert that it will do something yet dismiss the inevitable result as pure "speculati[on]." Def. Opp'n 6.

18-F-1517//1575

Third, the Commission's characterization of the data it seeks ("publicly available") is meaningless in the Article III standing context. The Commission has no legal authority to collect the personal voter data it has requested. *See* 44 U.S.C. § 3501 note. If it nevertheless collects that data, the Commission has broken the law and caused an injury in fact. *See CAIR*, 667 F. Supp. 2d at 76; *Hosp. Staffing Sols*, 736 F. Supp. 2d at 200. It does not matter that a particular state might disclose its voter data to some *other* requester under some *other* circumstances: *this* requester—the Commission—is barred by law from gathering this data without sufficient constitutional and statutory privacy safeguards. Nor can the Commission use the existing vulnerability of voter data at the state level to justify an even greater risk to voter privacy at the federal level. Def. Opp'n 7, ECF No. 8. A lesser harm does not excuse a greater one, and it certainly does not erase an injury in fact.

This Court consequently has jurisdiction to decide this case under Article III.

CONCLUSION

The Emergency Motion for a Temporary Restraining Order and Preliminary Injunction should be granted, and Defendants should be restrained from collecting state voter data prior to the completion of a Privacy Impact Assessment.

18-F-1517//1576

Respectfully Submitted,

/s/ Marc Rotenberg
MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel

CAITRIONA FITZGERALD*
EPIC Policy Director

JERAMIE D. SCOTT, D.C. Bar # 1025909
EPIC Domestic Surveillance Project Director

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Plaintiff EPIC

* *Pro hac vice motion pending*

Dated: July 17, 2017

18-F-1517//1577

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY; MICHAEL PENCE, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; KRIS KOBACH, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES; OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES; GENERAL SERVICES ADMINISTRATION Defendants.	Civ. Action No. 17-1320 (CKK)

DECLARATION BY ELENI KYRIAKIDES

I, Eleni Kyriakides, declare as follows:

1. My name is Eleni Kyriakides.

2. I am an EPIC Law Fellow at the Electronic Privacy Information Center.

3. In my capacity as a Fellow, I coordinate EPIC's Open Government Project. This includes overseeing EPIC's work using the Freedom of Information Act (FOIA).

4. EPIC makes frequent use of the FOIA to obtain records on government programs implicating privacy and civil liberties. EPIC seeks public disclosure of this information to help ensure that the public is fully informed about the activities of government, and to conduct oversight and analysis of these programs.

5. By refusing to release a Privacy Impact Assessment as required by law, the Defendants have increased the burden on EPIC to conduct its "oversight and analysis" in a more costly and resource-intensive way that would not otherwise be necessary.

6. As a result, I have researched, drafted, and submitted five requests seeking details related to the Commission's recent activities: one to the U.S. Department of Justice, two to the Commission, one to the General Services Administration, and one to the Arkansas Secretary of State Mark Martin. *See* EPIC Exhibit FOIA Requests.

I declare under penalty of perjury that, to the best of my knowledge, the forgoing is true and correct.

Executed July 17, 2017.

Respectfully Submitted,

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: July 17, 2017

18-F-1517//1579

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA E-MAIL

June 30, 2017

Nelson D. Hermilla, Chief
FOIA/PA Branch
Civil Rights Division
Department of Justice
BICN Bldg., Room 3234
950 Pennsylvania Avenue, NW
Washington, DC 20530
CRT.FOIArequests@usdoj.gov

Dear Mr. Hermilla,

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Department of Justice ("DOJ").

On June 28, 2017, the DOJ wrote to all states covered by the National Voter Registration Act ("NVRA") with a sweeping request for information regarding state voter registration list maintenance including "All statutes, regulations, written guidance, internal policies, or database user manuals that set out the procedures" the states have in place related to voter registration requirements, any other relevant procedures, and an explanation of the officials responsible for maintaining voter registration lists. The DOJ also sought, for local election officials, descriptions of the steps taken to ensure list maintenance is in "full compliance with the NVRA."[1] The DOJ gave the states 30 days to comply with the request. The DOJ offered no explanation or justification for the unprecedented time-bound request, stating only that the agency "reviewing voter registration list maintenance procedures in each state covered by the NVRA."[2]

Also on June 28, 2017, the Kris Kobach, the Vice Chair of the Presidential Advisory Commission on Election Integrity ("PACIE"), sent a letter to the Secretaries of State for all 50 states and the District of Columbia asking that the states provide the Commission detailed voter information, including

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony

[1] *See, e.g.*, Letter from T. Christian Herren, Jr., Chief, Voting Section, U.S. Dep't ment of Justice, to Kim Westbrook Strach, Exec. Dir., North Carolina State Bd. Of Elections (June 28, 2017), https://www.documentcloud.org/documents/3881855-Correspondence-DOJ-Letter-06282017.html.
[2] *Id.*

convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.[3]

EPIC seeks two categories of records concerning the DOJ's June 28th request for information on state voter list procedures.

Records Requested

(1) All records, including memoranda, legal analyses, and communications, concerning the DOJ's June 28, 2017 request to the states regarding voter list maintenance; and

(2) All communications between the DOJ and the Presidential Advisory Commission on Election Integrity ("PACEI") regarding the June 28, 2017 PACEI request for state voter data as well as any legal memoranda concerning the authorities of the PACEI.

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request. 5 U.S.C. § 552(a)(6)(E)(v)(II). To warrant expedited processing, under DOJ FOIA regulations a FOIA request must concern a matter of (1) "urgency to inform the public about an actual or alleged federal government activity," and, (2) the request must be "made by a person who is primarily engaged in disseminating information." 28 C.F.R. § 16.5(e)(1)(ii). This request satisfies both requirements.

First, there is an "urgency to inform the public about an actual or alleged federal government activity." § 16.5(e)(1)(ii). The "actual…federal government activity" at issue is DOJ's request to the states covered by the National Voter Registration Act ("NVRA") for information concerning each state's "voter registration list maintenance procedures." The DOJ concedes this activity in letters to the states.[4]

"Urgency" to inform the public about this activity is clear given the extraordinary nature and unusual breadth of the DOJ's request. On June 28, 2017, DOJ requested that all states covered by the NVRA provide to the DOJ *within 30 days* a sweeping list of information about state voting list maintenance. Indeed, former DOJ civil rights official and professor Justin Levitt told *ProPublica* that "he did not recall a time when the DOJ has previously requested such broad information."[5] Former senior litigator with the DOJ's Voting Section, David Becker called the move "unprecedented":

---

[3] *See, e.g.* Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html; *See generally* EPIC, *Voter Privacy and the PACEI,* https://epic.org/privacy/voting/pacei/.

[4] *Id.*

[5] *Jessica Huseman, Presidential Commission Demands Massive Amounts of State Voter Data*, ProPublica (June 29, 2107), https://www.propublica.org/article/presidential-commission-demands-massive-amounts-of-state-voter-data.

> In the quarter-century since passage of the NVRA, of which I spent seven years as a DOJ lawyer enforcing the NVRA, among other laws, *I do not know of the DOJ conducting any other broad-based fishing expedition into list maintenance compliance, whether during Democratic or Republican administrations.*[6]

Former deputy assistant general for civil rights Sam Bagnestos warned: "Let's be clear about what this letter signals: DOJ Civil Rights is preparing to sue states to force them to trim their voting rolls."[7]

The DOJ's request also represents a selective review of state voting processes,[8] without any basis offered for its narrow focus. The NVRA was passed not only to ensure "accurate and current voter registration rolls," but also "to establish procedures that will increase the number of eligible citizens who register to vote in elections for Federal office" and recognized that "the right of citizens of the United States to vote is a fundamental right." 52 U.S.C. § 20501. For instance, the DOJ request did not include an information request for compliance NVRA requirements voter registration forms be made easily available for distribution (§ 20505(b)), for simultaneous voter registration while applying for a driver's license (§ 20505(a)), and that state offices that provide public assistance and services to those with disabilities provide voter registration application forms and assistance (§ 20505(a)(4)(A)).

Despite the extraordinary nature of the request the DOJ offered no explanation or justification for the sudden broad-based request. The DOJ merely cited an agency review of "voter registration list maintenance procedures" in these states,[9] and "did not respond to requests for comment about the letters."[10]

States have thirty days to respond to the DOJ request. There is an urgent public need for immediate release of information explaining the DOJ's unprecedented decision to demand this voting list information from states. Moreover, the coincidental request by the PACEI for similar information from the states raises substantial concerns that the DOJ request was part of a coordinated undertaking. The PACEI has given the states approximately two weeks to respond their request.

Second, EPIC is an organization "primarily engaged in disseminating information." § 16.5(e)(1)(ii). As the Court explained in *EPIC v. Dep't of Def.*, "EPIC satisfies the definition of

---

[6] David Becker, *Why Wednesday's 'Election Integrity' Actions Should Be Watched By States*, Route Fifty (June 29, 2017), http://www.routefifty.com/management/2017/06/trump-election-integrity-commission-state-voter-data/139107/ (emphasis added).
[7] @sbagen, Twitter (June 29, 2017, 1:46 PM), https://twitter.com/sbagen/status/880528035392491520.
[8] *Jessica Huseman*, *supra* note 6.
[9] *See* Letter from T. Christian Herren, Jr. to Kim Westbrook Strach, Exec. Dir., North Carolina State Bd. Of Elections, *supra* note 1.
[10] *Id.*

'representative of the news media'" entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because disclosure of the requested information "is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest" of EPIC. 28 C.F.R. § 16.10(k)(1); § 552(a)(4)(A)(iii). EPIC's request satisfies the FBI's three factors for granting a fee waiver. § 16.10(k)(2).

Under the DOJ FOIA regulations, DOJ components evaluate three considerations to determine whether fee waiver is warranted: (i) the "subject of the request must concern identifiable operations or activities of the Federal Government with a connection that is direct and clear, not remote or attenuated"; (ii) disclosure must be "likely to contribute significantly to public understanding of those operations or activities"; and (iii) "disclosure must not be primarily in the commercial interest of the requester." §§ 16.10(k)(2)(i)–(iii).

First, disclosure of the requested DOJ records concerning the June 28th request to states for "voter registration list maintenance" self-evidently "concerns identifiable operations or activities of the Federal Government with a connection that is direct and clear, not remote or attenuated." § 16.10(k)(2)(i). This request concerns a direct request from the DOJ to states for information, concerning a law that the DOJ is authorized to enforce.

Second, disclosure "would be likely to contribute significantly to public understanding of those operations or activities" according to the two sub-factors. § 16.10(k)(2)(ii)(A-B). As to the first sub-factor, disclosure would be "meaningfully informative about government operations or activities" because the justification and decision-making underlying for the DOJ's unprecedented request to states covered by the NVRA has not been made public. § 16.10(k)(2)(ii)(A). Any additional information about how why the DOJ is seeking broad based data under only select provisions of NVRA would thus be "meaningfully informative" about the DOJ request. As to the second sub-factor, disclosure will "contribute to the understanding of a reasonably broad audience of persons interested in the subject," because, as stated in the relevant FOIA regulations, components will "presume that a representative of the news media will satisfy this consideration." § 16.10(k)(2)(ii)(B).

Third, disclosure of the requested information is not "primarily in the commercial interest" of EPIC according to the two sub-factors. § 16.10(k)(2)(iii)(A-B). As to the first sub-factor, EPIC

has no "commercial interest…that would be furthered by the requested disclosure." § 16.10(k)(2)(iii)(A). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[11] As to the second sub-factor, "the component must determine whether that is the primary interest furthered by the request" because, as stated in the FOIA regulations, DOJ "ordinarily will presume that where a news media requester has satisfied [the public interest standard], the request is not primarily in the commercial interest of the requester." § 16.10(k)(2)(iii)(B). As already described above, EPIC is a news media requester and satisfies the public interest standard.

For these reasons, a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. I anticipate your determination on our request within ten calendar days 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

[11] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.

epic.org
Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA
+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA E-Mail

July 4, 2017
Presidential Advisory Commission on Election Integrity
ElectionIntegrityStaff@ovp.eop.gov

Dear Sir or Madam:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Presidential Commission on Election Integrity ("PACEI" or "Commission").

This is a request for records in possession of the agency concerning the letters that were sent on or about June 28, 2017 requesting the production of state voter records and other related information.

Background

The Presidential Advisory Commission on Election Integrity was established by executive order on May 11, 2017.[1] On June 28, 2017, the Commission undertook an effort to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.[2]

The Vice Chair indicated that the Commission expected a response from the states by July 14, 2017.[3]

Such a request to state election officials had never been made by any federal official before. Election officials across the political spectrum in at least two dozen states have already partially or fully refused to comply with PACEI's request.[4]

---

[1] Exec. Order No. 13,799, 82 Fed. Reg. 22, 389 (May 11, 2017).
[2] Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Sec'y of State, North Carolina (June 28, 2017), https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html.
[3] *Id.*
[4] Philip Bump & Christopher Ingraham, *Trump Says States Are 'Trying to Hide' Things from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017),

On June 28th, the U.S. Department of Justice issued a parallel request. The DOJ wrote to all states covered by the National Voter Registration Act with a similarly unprecedented demand for information regarding compliance with state voter registration list maintenance.[5] The DOJ gave the states 30 days to comply with the request.

EPIC seeks nine categories of records from the agency concerning the Commission's June 28th, 2017 request to state election officials.

Records Requested

(1) All communications to state election officials regarding the request;

(2) All communications between and amongst Commission staff and Commission members regarding the request;

(3) All communications between the Commission staff and the Department of Justice and all communications between Commission members and the Department of Justice regarding the request;

(4) All records concerning compliance with the E-Government Act of 2002 and the specific obligation to undertake a Privacy Impact Assessment;

(5) All records concerning compliance with the Federal Advisory Committee Act and the failure to post a Privacy Impact Assessment;

(6) All records concerning compliance with the Privacy Act of 1974 and the failure to undertake a Systems of Records Notice;

(7) All records concerning the decision to use an insecure website and an insecure email address to receive state voter data;

(8) All legal memorandum concerning the Commission's authority to request personal data from the states; and

(9) Such other records that assess the privacy and security risks of aggregating nearly two hundred million voter records in a federal database.

---

https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/?utm_term=.bd2ba9587f57.

[5] *See, e.g.*, Letter from T. Christian Herren, Jr., Chief, Voting Section, U.S. Dep't ment of Justice, to Kim Westbrook Strach, Exec. Dir., North Carolina State Bd. Of Elections (June 28, 2017), https://www.documentcloud.org/documents/3881855-Correspondence-DOJ-Letter-06282017.html.

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request. To warrant expedited processing, a FOIA request must concern a "compelling need." 5 U.S.C. § 552(a)(6)(E)(i). "Compelling need" is demonstrated where the request is (1) "made by a person primarily engaged in disseminating information," with (2) "urgency to inform the public concerning actual or alleged Federal Government activity." § 552(a)(6)(E)(v)(II). This request satisfies both requirements.

First, EPIC is an organization "primarily engaged in disseminating information." § 552(a)(6)(E)(v)(II). As the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media.'" 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

Second, there is an "urgency to inform the public about an actual or alleged Federal Government activity." § 552(a)(6)(E)(v)(II). The "actual…Federal Government activity" at issue is PACEI's request to states for detailed voter history information. The PACEI concedes this activity in letters to the states.[6]

"Urgency" to inform the public about this activity is clear given the extraordinary nature of PACEI's sweeping request for voter data.[7] On June 28, 2017, PACEI independently requested that fifty states and D.C. - within approximately *ten business days* – disclose sensitive, personal information that individuals are often required to provide to be eligible to vote. To date, PACEI has not indicated how the information will be used, who will have access to it, or what safeguards will be established. PACEI has also not made any Privacy Impact Assessment for the collection of state voter data.

As noted already, state officials in over two dozen states have partially or fully opposed PACEI's demand.[8] Mississippi Secretary of State Delbert Hosemann stated, "They can go jump in the Gulf of Mexico."[9] California Secretary of State Alex Padilla added that he would "not provide sensitive voter information to a committee that has already inaccurately passed judgment that millions of Californians voted illegally. California's participation would only serve to legitimize the false and already debunked claims of massive voter fraud."[10] Kentucky's Secretary of State

---

[6] *See* Letter from Kris Kobach to Elaine Marshall, *supra* note 2.
[7] *Voter Privacy and the PACEI*, Epic.org, https://epic.org/privacy/voting/pacei/.
[8] *See* Philip Bump & Christopher Ingraham, *supra* note 4.
[9] Editorial Board, *Happy Fourth of July! Show Us Your Papers*, N.Y. Times (July 3, 2017), https://mobile.nytimes.com/2017/07/03/opinion/voter-fraud-data-kris-kobach.html.
[10] Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017), http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/.

Alison Lundergan Grimes concluded, "There's not enough bourbon here in Kentucky to make this request seem sensible."[11]

Fifty technical experts and legal scholars and twenty organizations expert in election integrity, voting verification, and voter privacy also recorded opposition to PACEI's request. In a letter to state officials, they explained: "As custodians of voter data, you have a specific responsibility to safeguard voter record information."[12]

This request concerns a matter of widespread public concern; the right to vote is protected by the U.S. Constitution. U.S. Const. amends. XV, XIX, XXIV, XXVI. Voter privacy and the secret ballot are unquestionably integral to American democracy.

States have only days left to respond to PACEI's request. There is an urgent public need for immediate release of information explaining the PACEI's unprecedented decision to collect, en masse, voters' personal information from the states. Moreover, the coincidental request by the DOJ for similar information from the states raises substantial concerns that the PACEI request was part of a coordinated undertaking.[13]

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because disclosure of the requested information "is in the public interest" because (1) "it is likely to contribute significantly to public understanding of the operations or activities of the government," and (2) disclosure "is not primarily in the commercial interest" of EPIC. § 552(a)(4)(A)(iii).

First, disclosure of the requested PACEI records concerning the June 28th request to states for detailed voter histories "is likely to contribute significantly to public understanding of the operations or activities of the government." § 552(a)(4)(A)(iii). The requested PACEI records self-evidently concerns "operations or activities of the government." *Id.* This request concerns a direct

---

[11] Max Greenwood, *Kentucky secretary of state: 'Not enough bourbon in Kentucky' to make me release voter data*, Hill (June 30, 2017), http://thehill.com/homenews/state-watch/340331-kentucky-secretary-of-state-not-enough-bourbon-in-kentucky-to-make-me.

[12] Letter from Organizations and Individual Experts to National Association of State Secretaries (July 3, 2017), https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf.

[13] *See* Letter from Eleni Kyriakides, EPIC Law Fellow, to Nelson Hermilla, Chief, FOIA/PA Branch, Civil Rights Div. (June 30, 2017), https://epic.org/privacy/voting/EPIC-17-06-30-DOJ-20170630-Request.pdf

request from a presidential commission to state officials to obtain state voter information. Disclosure of the PACEI records is also "likely to contribute significantly to public understanding" of the Commission's activities because, despite the extraordinary nature of PACEI's demand, the Commission has not explained how it plans to use, protect, or dispose of the sensitive personal data requested. § 552(a)(4)(A)(iii). Any additional information about how and why PACEI is seeking this data would "contribute significantly" to the public's understanding of PACEI's activities.

Second, disclosure of the requested information is not "primarily in the commercial interest" of EPIC. § 552(a)(4)(A)(iii). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[14]

For these reasons, a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. I anticipate your determination on our request within ten calendar days 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

[14] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA MAIL & FOIAonline

June 12, 2017

U.S. General Services Administration
FOIA Requester Service Center (H1F)
1800 F Street, NW, Room 7308
Washington, DC 20405-0001

Dear Sir/Madam,

This letter constitutes an urgent request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the General Services Administration ("GSA").

EPIC seeks records in possession of the agency concerning the transfer of voter data from the State of Arkansas to the Department of Defense following the June 28, 2017 letter from the Presidential Advisory Commission on Election Integrity (the "Commission").

Background

On June 28, 2017, the Vice Chair of the Commission attempted to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information. [1]

The letter provides no indication that the Commission will pay fees for the receipt voter data. The Commission also indicated a website for the transmission of voter data, which has since been determined to be insecure for the receipt of personally identifiable information from the general public.[2] Further, the letter from the Commission indicated no familiarity with the data that may disclosed by a particular state that received the request or the procedures the Commission would be required to follow to obtain voter data from a particular state.

---

[1] *See, e.g.* Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html.

[2] Lewis Decl. Ex. 11., EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

Following a proceeding brought by EPIC, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017) on July 7, 2017 the U.S. Department of Justice told the D.C. District Court that Arkansas transferred voter data, to the Department of Defense's SAFE Website, following the letter from the Vice Chair.[3]

The Arkansas Secretary of State's Office charges $2.50 per statewide voter registration data file.[4] A requesting party also completes a "Data Request Form" in order to obtain the file and must mail payment (in check or money order form) to the Arkansas Secretary of State offices.[5] The Office provides three types of files, with three clearly defined sets of information:

> (1) "…Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted."
>
> (2) "Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle" while "older elections are incomplete since some counties did not enter voter results into the previously used VR databases." And
>
> (3) "…a combination of the Voter Registration and Vote History files (VRVH)."[6]

The files are provided in ".CSV format" and "are available in CD format for pickup at the State Capitol Building or by mail" or "can also be placed on an FTP site."[7]

EPIC seeks four categories of records from the agency concerning the Arkansas transfer of data to the Commission.

Records Requested

> (1) All records indicating payment by the Commission to obtain Arkansas voter records;
>
> (2) The completed "Data Request Forms," prepared by the Commission to obtain the Arkansas state vote records;
>
> (3) All records indicating the types of data transferred by Arkansas to the Commission; and

---

[3] Transcript of Temporary Restraining Order at 40, EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).
[4] *Voter Data Request Form*, Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/Data%20Request%20Form.pdf (last visited July 12, 2017).
[5] *Id.*
[6] *Id.*
[7] *Id.*

(4) All records indicating the Commission's compliance with the Arkansas procedures to obtain state voter records.

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request because this request involves a "compelling need." 5 U.S.C. § 552(a)(6)(E)(i). Specifically, under GSA FOIA regulations a request warrants expedited processing where the information sought is (1) "urgently needed," (2) "by an individual primarily engaged in disseminating information," and (3) "in order to inform the public concerning actual or alleged Federal Government activity." 41 C.F.R. § 105-60.402-2(c)(2). This request satisfies all three requirements.

First, records concerning the Arkansas voter data transfer to the SAFE website, obtained following the June 28th request, is "urgently needed." § 105-60.402-2(c)(2). This information "has a particular value that will be lost if not disseminated quickly." *Id.* Indeed, this request concerns *both* a "breaking news story" and an issue of significant "general public interest." *Id.* On June 28, 2017, PACEI independently requested that fifty states and D.C. - within approximately *ten business days* – disclose sensitive, personal information individuals are often required to provide to be eligible to vote. Since that date, public interest in the PACEI's demand for state election officials to transfer personal voter data has dominated the news cycle, driven by prompt dissent of state officials in at least two dozen states across the political spectrum and public outcry.[8] Following PACEI's request less than two weeks ago, "[t]en states noted at least a slight increase in citizen calls and emails, and some citizens inquired about the process to unregister to vote, or how to secure their personal information."[9]

On July 7th, in a hearing before the D.C. District Court, the DOJ first revealed that Arkansas alone had transferred personal data to the Commission.[10] There are approximately 1.7 million registered voters in the state of Arkansas potentially implicated by this transfer.[11] The Commission will hold its first meeting on July 19, 2017.[12] Ahead of that meeting, the public must know whether the Commission and Arkansas state officials complied with state procedures in transferring this sensitive personal data.

---

[8] Philip Bump & Christopher Ingraham, *Trump Says States Are 'Trying to Hide' Things from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/?utm_term=.bd2ba9587f57.

[9] Dylan Wells & Saisha Talwar, *Some voters un-registering following Trump administration's data requests*, ABC News (July 11, 2017), http://abcnews.go.com/Politics/voters-registering-trump-administrations-data-requests/story?id=48578555.

[10] Transcript of Temporary Restraining Order at 40, *supra* note 3.

[11] *Registered Voters [As of 6/1/16]*, Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/ARRegisteredVoters6-1-16.pdf (last visited July 12, 2017).

[12] Meeting notice, 82 FR 31063 (July 5, 2017).

Second, EPIC is an organization "primarily engaged in disseminating information," § 105-60.402-2(c)(2). As the Court explained in *EPIC v. Dep't of Def.*, "EPIC satisfies the definition of 'representative of the news media'" entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

Third, this request involves "actual…federal government activity." § 105-60.402-2(c)(2). This FOIA concerns PACEI's request to states for detailed voter history information, conceded by PACEI in letters to the states,[13] and the transfer of Arkansas voter data to PACEI via the SAFE website, conceded by the DOJ to the D.C. District Court.[14]

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 105-60.402-2(c); § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II); 41 C.F.R. § 105-60.305-10(d)(2).

Further, any duplication fees should also be waived because disclosure of the requested information "would contribute significantly to public's understanding of the operations or activities of the Government and would not be primarily in the commercial interest" of EPIC. § 105-60.305-13; § 552(a)(4)(A)(iii). The GSA evaluates four considerations to determine whether this standard is met: (1) "Whether the subject of the requested records concerns 'the operations or activities of the Government,'"(2) "Whether the disclosure is 'likely to contribute' to an understanding of Government operations or activities," (3) "Whether disclosure of the requested information will contribute to [the] 'public's understanding,'" and (4) "Whether the requester has a commercial interest that would be furthered by the requested disclosure; and if so: whether the magnitude of the identified commercial interest of the requester is sufficiently large, in comparison with the public's interest in disclosure, that disclosure is 'primarily in the commercial interest of the requester.'" § 105-60.305-13(a)(1-4). EPIC's request satisfies these four GSA considerations for granting a fee waiver. § 105-60.305-13(a)(1-4).

First, disclosure of the requested GSA records concerning Arkansas transfer of voter data following PACEI's June 28th request self-evidently concerns "the operations or activities of the Government." § 105-60.305-13(a)(1). This request involves a direct request from a presidential commission to a state officials to obtain state voter information, and the transfer of data to a federal website following that request.

Second, "disclosure is 'likely to contribute' to an understanding of Government operations or activities." § 105-60.305-13(a)(2). The requested information about the Arkansas data transfer is

[13] *See* Letter from Kris Kobach to Elaine Marshall, *supra* note 1.
[14] Transcript of Temporary Restraining Order at 40, *supra* note 3.

not "already in the public domain." *Id.* Few details surrounding the transfer have been disclosed to the public, and the existence of the transfer was first made public mere days ago.

Third, "disclosure of the requested information will contribute to [the] 'public's understanding" § 105-60.305-13(a)(3). As stated in the GSA FOIA regulations, the "identity and qualifications of the requester should be considered to determine whether the requester is in a position to contribute to public's understanding through the requested disclosure." *Id.* As already indicated, EPIC is a news media requester. EPIC regularly disseminates information obtained through the FOIA as a part of its public interest mission through website EPIC.org, a bi-weekly "EPIC Alert," and other publications.[15]

Fourth, EPIC has no "commercial interest that would be furthered by the requested disclosure." § 105-60.305-13(a)(4). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[16]

For these reasons, a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. I anticipate your decision concerning EPIC's request for expedited processing within five working days. 41 C.F.R. § 105-60.402-2(d). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

[15] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.
[16] *Id.*

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA E-Mail

July 12, 2017
Presidential Advisory Commission on Election Integrity
ElectionIntegrityStaff@ovp.eop.gov

Dear Sir or Madam:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Presidential Commission on Election Integrity (the "Commission").

EPIC seeks records in possession of the agency concerning the transfer of voter data from the State of Arkansas to the Department of Defense following the June 28, 2017 Commission letter.

Background

On June 28, 2017, the Vice Chair of the Commission attempted to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information. [1]

The letter provides no indication that the Commission will pay fees for the receipt voter data. The Commission also indicated a website for the transmission of voter data, which has since been determined to be insecure for the receipt of personally identifiable information from the general public.[2] Further, the letter from the Commission indicated no familiarity with the data that may disclosed by a particular state that received the request or the procedures the Commission would be required to follow to obtain voter data from a particular state.

Following the proceeding brought by EPIC, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017) on July 7, 2017 the U.S. Department of Justice told the D.C. District Court that

---

[1] *See, e.g.* Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html.

[2] Lewis Decl. Ex. 11., EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

Arkansas transferred voter data, to the Department of Defense's SAFE Website, following the letter from the Vice Chair.[3]

The Arkansas Secretary of State's Office charges $2.50 per statewide voter registration data file.[4] A requesting party also completes a "Data Request Form" in order to obtain the file and must mail payment (in check or money order form) to the Arkansas Secretary of State offices.[5] The Office provides three types of files, with three clearly defined sets of information:

> (1) "…Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted."
>
> (2) "Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle" while "older elections are incomplete since some counties did not enter voter results into the previously used VR databases." And
>
> (3) "…a combination of the Voter Registration and Vote History files (VRVH)."[6]

The files are provided in ".CSV format" and "are available in CD format for pickup at the State Capitol Building or by mail" or "can also be placed on an FTP site."[7]

EPIC seeks four categories of records from the agency concerning the Arkansas transfer of data to the Commission.

Records Requested

> (1) All records indicating payment by the Commission to obtain Arkansas voter records;
>
> (2) The completed "Data Request Forms," prepared by the Commission to obtain the Arkansas state vote records;
>
> (3) All records indicating the types of data transferred by Arkansas to the Commission; and
>
> (4) All records indicating the Commission's compliance with the Arkansas procedures to obtain state voter records.

---

[3] Transcript of Temporary Restraining Order at 40, EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).
[4] *Arkansas Voter Registration Data*, Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/Data%20Request%20Form.pdf (last visited July 12, 2017).
[5] *Id.*
[6] *Id.*
[7] *Id.*

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request. To warrant expedited processing, a FOIA request must concern a "compelling need." 5 U.S.C. § 552(a)(6)(E)(i). "Compelling need" is demonstrated where the request is (1) "made by a person primarily engaged in disseminating information," with (2) "urgency to inform the public concerning actual or alleged Federal Government activity." § 552(a)(6)(E)(v)(II). This request satisfies both requirements.

First, EPIC is an organization "primarily engaged in disseminating information." § 552(a)(6)(E)(v)(II). As the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media.'" 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

Second, there is an "urgency to inform the public about an actual or alleged Federal Government activity." § 552(a)(6)(E)(v)(II). The "actual…Federal Government activity" at issue PACEI's request to states for detailed voter history information, conceded by PACEI in letters to the states,[8] and the transfer of Arkansas voter data to PACEI via the SAFE website, conceded by the DOJ in D.C. District Court.[9]

"Urgency" to inform the public about the Arkansas voter data transfer to the SAFE website, following the Commission's June 28th request. On June 28, 2017, PACEI independently requested that fifty states and D.C. - within approximately *ten business days* – disclose sensitive, personal information individuals are often required to provide to be eligible to vote. Since that date, public interest in the PACEI's demand for state election officials to transfer personal voter data has dominated the news cycle, driven by prompt dissent of state officials in at least two dozen states across the political spectrum and public outcry.[10] Following PACEI's request less than two weeks ago, "[t]en states noted at least a slight increase in citizen calls and emails, and some citizens inquired about the process to unregister to vote, or how to secure their personal information."[11]

On July 7th, in a hearing before the D.C. District Court, the DOJ first revealed that Arkansas alone had transferred personal data to the Commission.[12] There are approximately 1.7

---

[8] *See* Letter from Kris Kobach to Elaine Marshall, *supra* note 1.
[9] Transcript of Temporary Restraining Order at 40, *supra* note 3.
[10] Philip Bump & Christopher Ingraham, *Trump Says States Are 'Trying to Hide' Things from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/?utm_term=.bd2ba9587f57.
[11] Dylan Wells & Saisha Talwar, *Some voters un-registering following Trump administration's data requests*, ABC News (July 11, 2017), http://abcnews.go.com/Politics/voters-registering-trump-administrations-data-requests/story?id=48578555.
[12] Transcript of Temporary Restraining Order at 40, *supra* note 3.

million registered voters in the state of Arkansas potentially implicated by this transfer.[13] The Commission will hold its first meeting on July 19, 2017.[14] Ahead of that meeting, the public must know whether the Commission and Arkansas state officials complied with state procedures in transferring this sensitive personal data.

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because disclosure of the requested information "is in the public interest" because (1) "it is likely to contribute significantly to public understanding of the operations or activities of the government," and (2) disclosure "is not primarily in the commercial interest" of EPIC. § 552(a)(4)(A)(iii).

First, disclosure of the requested PACEI records concerning the Arkansas voter data transfer "is likely to contribute significantly to public understanding of the operations or activities of the government." § 552(a)(4)(A)(iii). The requested PACEI records self-evidently concerns "operations or activities of the government." *Id.* This request involves a direct request from a presidential commission to a state officials to obtain state voter information, and the transfer of data to a federal website following that request. Disclosure of the PACEI records is also "likely to contribute significantly to public understanding" of the Commission's activities because, the requested information about the Arkansas data transfer is not "already in the public domain." *Id.* Few details surrounding the transfer have been disclosed to the public. Indeed, the existence of the transfer was first made public mere days ago. Any additional information about the circumstances of the data transfer would there "contribute significantly" to the public's understanding of PACEI's activities. *Id.*

Second, disclosure of the requested information is not "primarily in the commercial interest" of EPIC. § 552(a)(4)(A)(iii). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[15]

For these reasons, a fee waiver should be granted.

---

[13] *Registered Voters [As of 6/1/16],* Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/ARRegisteredVoters6-1-16.pdf (last visited July 12, 2017).
[14] Meeting notice, 82 FR 31063 (July 5, 2017).
[15] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.

Conclusion

Thank you for your consideration of this request. I anticipate your decision concerning EPIC's request for expedited processing within ten calendar days. 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA MAIL

July 13, 2017

The Honorable Mark Martin
Secretary of State
ATTN: FOIA Officer
256 State Capitol
500 Woodlane Street
Little Rock, AR 72201

Dear Sir or Madam:

This letter constitutes a request under the Arkansas Freedom of Information Act Ark. Code Ann. § 25-19-105(a)(2)(A) (1967) to receive copies of records, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Office of Arkansas Secretary of State Mark Martin.

EPIC seeks records in possession of the Office concerning the transfer of voter data from the State of Arkansas to the Department of Defense following the June 28, 2017 Commission letter.

EPIC does not assert a claim to Arkansas records as a citizen of the state. § 25-19-105(a)(1)(A). Rather, EPIC urges the Secretary of State to publicly release the requested records in light of the profound public interest favoring release. "The generation that made the nation thought secrecy in government one of the instruments of Old World tyranny and committed itself to the principle that a democracy cannot function unless the people are permitted to know what their government is up to." *EPA v. Mink*, 410 U.S. 73, 105 (1973) (Douglas, W. dissenting) (quoting from The New York Review of Books, Oct. 5, 1972, p. 7). Transparency secures "informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *NLRB v. Robbins Tire & Rubber Co.,* 437 U.S. 214, 242 (1978). Here, EPIC seeks records concerning the Arkansas transfer of state voter data to the federal government in the pursuit of this overriding public interest.

Background

On June 28, 2017, the Vice Chair of the Commission attempted to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions,

information regarding voter registration in another state, information regarding military status, and overseas citizen information. [1]

The letter provides no indication that the Commission will pay fees for the receipt voter data. The Commission also indicated a website for the transmission of voter data, which has since been determined to be insecure for the receipt of personally identifiable information from the general public.[2] Further, the letter from the Commission indicated no familiarity with the data that may disclosed by a particular state that received the request or the procedures the Commission would be required to follow to obtain voter data from a particular state.

Following the proceeding brought by EPIC, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017) on July 7, 2017 the U.S. Department of Justice told the D.C. District Court that Arkansas transferred voter data, to the Department of Defense's SAFE Website, following the letter from the Vice Chair.[3]

The Arkansas Secretary of State's Office charges $2.50 per statewide voter registration data file.[4] A requesting party also completes a "Data Request Form" in order to obtain the file and must mail payment (in check or money order form) to the Arkansas Secretary of State offices.[5] The Office provides three types of files, with three clearly defined sets of information:

(1) "…Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted."

(2) "Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle" while "older elections are incomplete since some counties did not enter voter results into the previously used VR databases." And

(3) "…a combination of the Voter Registration and Vote History files (VRVH)."[6]

---

[1] *See, e.g.* Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html.

[2] Lewis Decl. Ex. 11., EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

[3] Transcript of Temporary Restraining Order at 40, EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

[4] *Arkansas Voter Registration Data*, Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/Data%20Request%20Form.pdf (last visited July 12, 2017).

[5] *Id.*

[6] *Id.*

The files are provided in ".CSV format" and "are available in CD format for pickup at the State Capitol Building or by mail" or "can also be placed on an FTP site."[7]

EPIC seeks four categories of records from the agency concerning the Arkansas transfer of data to the Commission.

Records Requested

(1) All records indicating payment by the Commission to obtain Arkansas voter records;

(2) The completed "Data Request Forms," prepared by the Commission to obtain the Arkansas state vote records;

(3) All records indicating the types of data transferred by Arkansas to the Commission; and

(4) All records indicating the Commission's compliance with the Arkansas procedures to obtain state voter records.

Request for Fee Waiver

EPIC requests that copies of the records "be furnished without charge or at a reduced charge" because (1) the records "have been requested primarily for noncommercial purposes," and (2) "waiver or reduction of the fee is in the public interest." § 25-19-105(d)(3)(A)(iv).

First, disclosure of the records "have been requested primarily for noncommercial purposes. § 25-19-105(d)(3)(A)(iv). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[8]

Second, "waiver or reduction of the fee is in the public interest." § 25-19-105(d)(3)(A)(iv). The requested records concern a matter of profound public interest: the transfer of Arkansas voters' data a Presidential commission. Nonetheless, there are few public details about the circumstances surrounding the transfer, and, indeed, the mere fact of the transfer was first made public only days ago.[9] On July 7th, in a hearing before the D.C. District Court, the DOJ first revealed that Arkansas alone had transferred personal data to the Commission.[10] There are approximately 1.7 million registered voters in the state of Arkansas potentially implicated by this transfer.[11] The Commission will hold its first meeting on July 19, 2017.[12] Ahead of that meeting,

---

[7] *Id.*

[8] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.

[9] Transcript of Temporary Restraining Order at 40, EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

[10] *Id.*

[11] *Registered Voters [As of 6/1/16],* Arkansas.gov http://www.sos.arkansas.gov/elections/Documents/ARRegisteredVoters6-1-16.pdf (last visited July 12, 2017).

the public must know whether the Commission and Arkansas state officials complied with state procedures in transferring this sensitive personal data.

For these reasons, a full fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org. EPIC anticipates your response within a maximum of three working days. § 25-19-105(e).

EPIC requests receipt of responsive records via e-mail, and, if not "readily convertible" to electronic format, in physical copies via mail to the 1718 Connecticut Ave. NW, Suite 200, Washington, DC 20009. § 25-19-105(d)(2)(B).

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

[12] Meeting notice, 82 FR 31063 (July 5, 2017).

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009

Plaintiff,

v.

Civ. Action No. 17-1320 (CKK)

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY; MICHAEL PENCE, in his official capacity as Chair of the Presidential Advisory Commission on Election Integrity; KRIS KOBACH, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; CHARLES C. HERNDON, in his official capacity as Director of White House Information Technology; EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES; OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES; UNITED STATES DIGITAL SERVICE; EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY;
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

GENERAL SERVICES ADMINISTRATION
1800 F Street, N.W.
Washington, D.C. 20405

UNITED STATES DEPARTMENT OF DEFENSE
1000 Defense Pentagon
Washington, D.C. 20301-0001

Defendants.

SECOND AMENDED COMPLAINT FOR INJUNCTIVE RELIEF

18-F-1517//1604

1. This is an action under the Administrative Procedure Act ("APA"), 5 U.S.C. §§ 551–706, the Federal Advisory Committee Act ("FACA"), 5 U.S.C. app. 2, and the United States Constitution for injunctive and other appropriate relief to halt the collection of state voter data by the Presidential Advisory Commission on Election Integrity (the "PACEI" or the "Commission"), by officers of the Commission, and by the agencies which oversee and facilitate the activities of the Commission, including the Department of Defense.

2. The Electronic Privacy Information Center ("EPIC") challenges the Defendants' intent to collect the personal data of millions of registered voters and to publish partial SSNs as an unconstitutional invasion of privacy and a violation of the obligation to conduct a Privacy Impact Assessment ("PIA").

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, 5 U.S.C. § 702, and 5 U.S.C. § 704. This Court has personal jurisdiction over Defendants.

4. Venue is proper in this district under 5 U.S.C. § 703 and 28 U.S.C. § 1391.

Parties

5. Plaintiff EPIC is a nonprofit organization incorporated in Washington, D.C., and established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities. EPIC's Advisory Board members include distinguished experts in law, technology, public policy, and cybersecurity. EPIC has a long history of working to protect voter privacy and the security of election infrastructure. EPIC has specific expertise regarding the misuse of the Social Security Number ("SSN") and has sought stronger protections for the SSN for more than two decades.

6. EPIC's members include registered voters in California, the District of Columbia, Florida, Maryland, Massachusetts, Minnesota, New York, Pennsylvania, Texas, and Washington.

18-F-1517//1605

7. Defendant PACEI is an advisory committee of the U.S. government within the meaning of FACA, 5 U.S.C. app. 2 § 10. Defendant PACEI is also an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

8. Defendant Michael Pence is the Vice President of the United States and the Chair of the PACEI.

9. Defendant Kris Kobach is the Secretary of State of Kansas and the Vice Chair of the PACEI.

10. Defendant Charles C. Herndon is the Director of White House Information Technology.

11. Defendant Executive Office of the President of the United States ("EOP") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

12. Defendant U.S. Digital Service is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

13. Defendant Executive Committee for Presidential Information Technology consists of the following officials or their designees: the Assistant to the President for Management and Administration; the Executive Secretary of the National Security Council; the Director of the Office of Administration; the Director of the United States Secret Services; and the Director of the White House Military Office. The Executive Committee is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

14. Defendant Office of the Vice President of the United States ("OVP") is a subcomponent of EOP and an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

15. Defendant General Services Administration ("GSA") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701. The GSA is charged with providing the PACEI

18-F-1517//1606

"such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission . . . ." Ex. 1.[1]

16. Defendant United States Department of Defense ("DoD") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701. The DoD manages and controls the Safe Access File System ("SAFE").

Facts

The Commission's Unprecedented Collection of State Voter Data

17. The Commission was established by Executive Order on May 11, 2017 ("Commission Order"). Ex 1.[2]

18. The Commission is charged with "study[ing] the registration and voting processes used in Federal elections." Ex. 1.[3] The Commission Order contains no authority to gather personal data or to undertake investigations.[4]

19. On June 28, 2017, the Vice Chair of the Commission undertook to collect detailed voter histories from all fifty states and the District of Columbia. Such a request had never been made by any federal official in the history of the country. The Vice Chair stated during a phone call with Commission members that "a letter w[ould] be sent today to the 50 states and District of Columbia on behalf of the Commission requesting publicly-available data from state voter rolls . . . ." Ex. 2.[5]

---

[1] Exec. Order. No. 13,799, 82 Fed. Reg. 22,389, 22,390 (May 11, 2017).
[2] 82 Fed. Reg. at 22,389; *see also Voter Privacy and the PACEI*, EPIC.org (June 30, 2017), https://epic.org/privacy/voting/pacei/.
[3] 82 Fed. Reg. at 22,389.
[4] *See generally id.*
[5] Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017).

18-F-1517//1607

20. According to the U.S. Census, state voter rolls include the names, addresses, and other personally identifiable information of at least 157 million registered voters.[6]

21. One of the letters from the Commission, dated June 28, 2017, was sent to North Carolina Secretary of State Elaine Marshall. Ex. 3.[7]

22. In the letter ("Commission Letter"), the Vice Chair urged the Secretary of State to provide to the Commission the "full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information." Ex. 3.[8]

23. The Commission Letter also asked "[w]hat evidence or information [the state had] regarding instances of voter fraud or registration fraud" and "[w]hat convictions for election-related crimes ha[d] occurred in [the] state since the November 2000 federal election." Ex. 3.[9]

24. The Commission Letter stated that "any documents that are submitted to the full Commission w[ould] also be made available to the public." Ex. 3.[10]

25. The Commission asked for a response by July 14, 2017. Ex. 3.[11] The "SAFE" URL, recommend by the Commission for the submission of voter data, leads election officials to a non-

---

[6] U.S. Census Bureau, *Voting and Registration in the Election of November 2016* at tbl. 4a (May 2017), https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-580.html.
[7] Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017).
[8] *Id.* at 1–2.
[9] *Id.* at 1.
[10] *Id.* at 2.
[11] *Id.*

18-F-1517//1608

secure site. Regarding this website, Google Chrome states: "Your connection is not private. Attackers may be trying to steal your information from [the site proposed by the Commission] (for example, passwords, messages, or credit cards)." Ex. 4.[12]

26. As of July 7, 2017, the Department of Defense has received voter data from at least one state, Arkansas, in the SAFE system.

27. According to representations made by the Commission in the July 10, 2017 response, the Commission sent a "Follow-up Communication" to the states, requesting that the States not submit any data until this Court rules on EPIC's motion for a temporary restraining order.

28. The Follow-up Communication from the Commission to the States was not made public as would be required by the Federal Advisory Committee Act.

29. There is no public confirmation that all of the States received the Follow-up Communication from the Commission.

30. There is no public confirmation that the States that did receive the Follow-up Communication will comply.

31. According to representations made by the Commission in the July 10, 2017 response, the Director of White House Information Technology is "repurposing" a computer system to be used for collecting personal voter data.

32. On July 10, 2017, the Commission stated that it would not send further instructions about how to use the new system pending the Court's resolution of EPIC's motion for a temporary restraining order.

[12] Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Site (July 3, 2017 12:02 AM).

18-F-1517//1609

33. On July 10, 2017, the Commission stated that it would not download the data that Arkansas already transmitted via the DoD system, and that the data will be deleted from the site. There has been no confirmation that the data has been deleted.

The General Service Administration's Role in Providing Support to the Commission

34. The Executive Order provides that the GSA "shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis."[13]

35. The Commission Charter designates the GSA as the "Agency Responsible for Providing Support," and similarly orders that the GSA "shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis."[14]

36. The GSA routinely conducts and publishes Privacy Impact Assessments when it collects, maintains, and uses personal information on individuals.[15]

37. There is no authority in the Executive Order of the Commission Charter for any other entity to provide "administrative services," "facilities," or "equipment" to "carry out [the Commission's] mission."

Many States Oppose the Commission's Demand for Personal Voter Data

38. In less than three days following the release of the Commission Letter, election officials in twenty-four states said that they would oppose, partially or fully, the demand for personal voter data.[16]

---

[13] 82 Fed. Reg. at 22,390.
[14] Charter, Presidential Advisory Commission on Election Integrity ¶ 6.
[15] *Privacy Impact Assessments*, GSA (Apr. 13, 2017), https://www.gsa.gov/portal/content/102237.

18-F-1517//1610

39. California Secretary of State Alex Padilla stated that he would "not provide sensitive voter information to a committee that has already inaccurately passed judgment that millions of Californians voted illegally. California's participation would only serve to legitimize the false and already debunked claims of massive voter fraud."[17]

40. Kentucky Secretary of State Alison Lundergan Grimes stated that "Kentucky w[ould] not aid a commission that is at best a waste of taxpayer money and at worst an attempt to legitimize voter suppression efforts across the country."[18]

41. Virginia Governor Terry McAuliffe stated that he had "no intention of honoring [Kobach's] request."[19]

42. More than fifty experts in voting technology and twenty privacy organizations wrote to state election officials to warn that "[t]here is no indication how the information will be used, who will have access to it, or what safeguards will be established."[20]

Failure to Conduct a Privacy Impact Assessment

---

[16] Philip Bump & Christopher Ingraham, *Trump Says States Are 'Trying to Hide' Things from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/.

[17] Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017), http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/.

[18] Bradford Queen, Secretary Grimes Statement on Presidential Election Commission's Request for Voters' Personal Information, Kentucky (last accessed July 3, 2017) http://kentucky.gov/Pages/Activity-stream.aspx?n=SOS&prId=129.

[19] Terry McAuliffe, *Governor McAuliffe Statement on Request from Trump Elections Commission* (June 29, 2017), https://governor.virginia.gov/newsroom/newsarticle?articleId=20595.

[20] Letter from EPIC et al. to Nat'l Ass'n of State Sec'ys (July 3, 2017), https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf.

18-F-1517//1611

43. Under the E-Government Act of 2002,[21] any agency "initiating a new collection of information that (I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual" is required to complete a Privacy Impact Assessment ("PIA") before initiating such collection.[22]

44. The agency must "(i) conduct a privacy impact assessment; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."[23]

45. The Commission is an agency subject to the E-Government Act because it is an "establishment in the executive branch of the Government," a category which "includ[es] the Executive Office of the President."[24]

46. The Executive Office of the President is an agency subject to the E-Government Act.

47. The U.S. Digital Service is an agency subject to the E-Government Act.

48. The Director of White House Information Technology is subject to the E-Government Act.

49. The Director of White House Information Technology was established in 2015 and has "the primary authority to establish and coordinate the necessary policies and procedures for

[21] Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note).
[22] 44 U.S.C. § 3501 note ("Privacy Impact Assessments").
[23] *Id.*
[24] 44 U.S.C. § 3502(1).

18-F-1517//1612

operating and maintaining the information resources and information systems provided to the President, Vice President, and EOP."[25] This authority includes:

> providing "policy coordination and guidance for, and periodically review[ing], all activities relating to the information resources and information systems provided to the President, Vice President, and EOP by the Community, including expenditures for, and procurement of, information resources and information systems by the Community. Such activities shall be subject to the Director's coordination, guidance, and review in order to ensure consistency with the Director's strategy and to strengthen the quality of the Community's decisions through integrated analysis, planning, budgeting, and evaluating process.[26]

The Director may also "advise and confer with appropriate executive departments and agencies, individuals, and other entities as necessary to perform the Director's duties under this memorandum."[27]

50. The Director has the independent authority to oversee and "provide the necessary advice, coordination, and guidance to" the Executive Committee for Presidential Information Technology, which "consists of the following officials or their designees: the Assistant to the President for Management and Administration; the Executive Secretary of the National Security Council; the Director of the Office of Administration; the Director of the United States Secret Service; and the Director of the White House Military Office."[28]

51. A Privacy Impact Assessment for a "new collection of information" must be "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information."[29] The PIA must specifically address "(I) what information is to be

---

[25] Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology § 1, 2015 Daily Comp. Pres. Doc. 185 (Mar. 19, 2015), attached as Ex. 5.
[26] *Id.* § 2(c).
[27] *Id.* § 2(d).
[28] *Id.* § 3.
[29] 44 U.S.C. § 3501 note ("Privacy Impact Assessments").

18-F-1517//1613

collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and] (VI) how the information will be secured . . . ."[30]

52. Under the FACA, "records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by [an] advisory committee shall be available for public inspection and copying at a single location in the offices of the advisory committee or the agency to which the advisory committee reports until the advisory committee ceases to exist."[31]

53. None of the Defendants have conducted a Privacy Impact Assessment for the Commission's collection of state voter data.

54. None of the Defendants have ensured review of a PIA by any Chief Information Officer or equivalent official.

55. The Commission has not published a PIA or made such an assessment available for public inspection.

The DoD's Privacy Impact Assessment Does Not Permit
the Collection of Personal Information from The General Public

56. The DoD last approved a PIA for the Safe Access File Exchange system in 2015.[32]

57. The 2015 PIA indicates that the SAFE system may "collect, maintain, use and/or disseminate PII" about only "federal personnel and/or federal contractors."[33]

---

[30] *Id.*
[31] 5 U.S.C. app. 2 § 10(b).
[32] Army Chief Information Officer, U.S. Dep't of Def., *Privacy Impact Assessments* (April 27, 2016), http://ciog6.army.mil/PrivacyImpactAssessments/tabid/71/Default.aspx.
[33] EPIC Supp. Ex. 5, ECF No. 20-1, at 1.

18-F-1517//1614

58. The 2015 PIA specifically indicates that the SAFE system may not be used to "collect, maintain, use and/or disseminate PII" from "members of the general public."[34]

59. According to the 2015 PIA, the SAFE system may not be used to collect the data set out in the June 28, 2017, from Vice Chair Kobach, directing state election officials to provide voter roll data.

60. The DoD has not issued a PIA for the collection of personal data from the general public.

61. The DoD has not issued a PIA that would permit the receipt of data specified in the June 28, 2017, Kobach letter.

Count I

Violation of APA: Unlawful Agency Action

62. Plaintiff asserts and incorporates by reference paragraphs 1–42.

63. Defendants' collection of state voter data prior to creating, reviewing, and publishing a Privacy Impact Assessment, 44 U.S.C. § 3501 note, is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law under 5 U.S.C. § 706(2)(a) and short of statutory right under 5 U.S.C. § 706(2)(c).

64. Defendants' decision to initiate collection of voter data is a final agency action within the meaning of 5 U.S.C. § 704.

65. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions.

66. Plaintiff has exhausted all applicable administrative remedies.

Count II

Violation of APA: Agency Action Unlawfully Withheld

[34] EPIC Supp. Ex. 5, ECF No. 20-1, at 1.

18-F-1517//1615

67. Plaintiff asserts and incorporates by reference paragraphs 1–42.

68. Defendants have failed to create, review, and/or publish a privacy impact assessment for Defendants' collection of voter data, as required by 44 U.S.C. § 3501 note and 5 U.S.C. app. 2 § 10(b).

69. Defendants' failure to take these steps constitutes agency action unlawfully withheld or unreasonably delayed in violation of 5 U.S.C. § 706(1).

70. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

71. Plaintiff has exhausted all applicable administrative remedies.

Count III

Violation of FACA: Failure to Make Documents Available for Public Inspection

72. Plaintiff asserts and incorporates by reference paragraphs 1–42.

73. Defendants have failed to make available for public inspection a privacy impact assessment for the collection of voter data.

74. Defendants' failure to make available for public inspection a PIA required by law is a violation of 5 U.S.C. app. 2 § 10(b).

75. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

76. Plaintiff has exhausted all applicable administrative remedies.

Count IV

Violation of Fifth Amendment: Substantive Due Process/Right to Informational Privacy

77. Plaintiff asserts and incorporates by reference paragraphs 1–42.

18-F-1517//1616

78. Defendants, by seeking to assemble an unnecessary and excessive federal database of sensitive voter data from state records systems, have violated the informational privacy rights of millions of Americans, including members of the EPIC Advisory Board, guaranteed by the Due Process Clause of the Fifth Amendment. *See* U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

79. Plaintiff, as a representative of its members, is adversely affected and aggrieved by Defendants' actions.

Count V

Violation of Fifth Amendment: Procedural Due Process

80. Plaintiff asserts and incorporates by reference paragraphs 1–42.

81. Defendants, by seeking to assemble an unnecessary and excessive federal database of sensitive voter data from state records systems, have deprived EPIC's members of their liberty interest in avoiding the disclosure of personal matters. U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

82. Defendants have done so without providing notice to EPIC's members, without providing EPIC's members an opportunity to challenge the collection of their personal data, and without providing for a neutral decisionmaker to decide on any such challenges brought by EPIC's members.

83. Defendants have violated EPIC's members Fifth Amendment right to due process of law. U.S. Const. amend. V.

18-F-1517//1617

84. Plaintiff, as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

Requested Relief

WHEREFORE, Plaintiff requests that this Court:

A. Hold unlawful and set aside Defendants' authority to collect personal voter data from the states;

B. Order Defendants to halt collection of personal voter data;

C. Order Defendants to securely delete and properly disgorge any personal voter data collected or subsequently received;

D. Order Defendants to promptly conduct a privacy impact assessment prior to the collection of personal voter data;

E. Award EPIC costs and reasonable attorney's fees incurred in this action; and

F. Grant such other relief as the Court may deem just and proper.

Respectfully Submitted,

/s/ Marc Rotenberg
MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel

CAITRIONA FITZGERALD*
EPIC Policy Director

JERAMIE D. SCOTT, D.C. Bar # 1025909
EPIC Domestic Surveillance Project Director

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.

18-F-1517//1618

Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Plaintiff EPIC

** Pro hac vice motion pending*

Dated: July 11, 2017

18-F-1517//1619

Exhibit 5

Administration of Barack Obama, 2015

Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology
March 19, 2015

Memorandum for the Secretary of Defense, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the National Security Advisor, and the Director of the Office of Administration

Subject: Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to improve the information resources and information systems provided to the President, Vice President, and Executive Office of the President (EOP), I hereby direct the following:

Section 1. Policy. The purposes of this memorandum are to ensure that the information resources and information systems provided to the President, Vice President, and EOP are efficient, secure, and resilient; establish a model for Government information technology management efforts; reduce operating costs through the elimination of duplication and overlapping services; and accomplish the goal of converging disparate information resources and information systems for the EOP.

This memorandum is intended to maintain the President's exclusive control of the information resources and information systems provided to the President, Vice President, and EOP. High-quality, efficient, interoperable, and safe information systems and information resources are required in order for the President to discharge the duties of his office with the support of those who advise and assist him, and with the additional assistance of all EOP components. The responsibilities that this memorandum vests in the Director of White House Information Technology, as described below, have been performed historically within the EOP, and it is the intent of this memorandum to continue this practice.

The Director of White House Information Technology, on behalf of the President, shall have the primary authority to establish and coordinate the necessary policies and procedures for operating and maintaining the information resources and information systems provided to the President, Vice President, and EOP. Nothing in this memorandum may be construed to delegate the ownership, or any rights associated with ownership, of any information resources or information systems, nor of any record, to any entity outside of the EOP.

Sec. 2. Director of White House Information Technology. (a) There is hereby established the Director of White House Information Technology (Director). The Director shall be the senior officer responsible for the information resources and information systems provided to the President, Vice President, and EOP by the Presidential Information Technology Community (Community). The Director shall:

(i) be designated by the President;

(ii) have the rank and status of a commissioned officer in the White House Office; and

18-F-1517//1621

(iii) have sufficient seniority, education, training, and expertise to provide the necessary advice, coordination, and guidance to the Community.

(b) The Deputy Chief of Staff for Operations shall provide the Director with necessary direction and supervision.

(c) The Director shall ensure the effective use of information resources and information systems provided to the President, Vice President, and EOP in order to improve mission performance, and shall have the appropriate authority to promulgate all necessary procedures and rules governing these resources and systems. The Director shall provide policy coordination and guidance for, and periodically review, all activities relating to the information resources and information systems provided to the President, Vice President, and EOP by the Community, including expenditures for, and procurement of, information resources and information systems by the Community. Such activities shall be subject to the Director's coordination, guidance, and review in order to ensure consistency with the Director's strategy and to strengthen the quality of the Community's decisions through integrated analysis, planning, budgeting, and evaluation processes.

(d) The Director may advise and confer with appropriate executive departments and agencies, individuals, and other entities as necessary to perform the Director's duties under this memorandum.

Sec. 3. Executive Committee for Presidential Information Technology. There is hereby established an Executive Committee for Presidential Information Technology (Committee). The Committee consists of the following officials or their designees: the Assistant to the President for Management and Administration; the Executive Secretary of the National Security Council; the Director of the Office of Administration; the Director of the United States Secret Service; and the Director of the White House Military Office.

Sec. 4. Administration. (a) The President or the Deputy Chief of Staff for Operations may assign the Director and the Committee any additional functions necessary to advance the mission set forth in this memorandum.

(b) The Committee shall advise and make policy recommendations to the Deputy Chief of Staff for Operations and the Director with respect to operational and procurement decisions necessary to achieve secure, seamless, reliable, and integrated information resources and information systems for the President, Vice President, and EOP. The Director shall update the Committee on both strategy and execution, as requested, including collaboration efforts with the Federal Chief Information Officer, with other government agencies, and by participating in the Chief Information Officers Council.

(c) The Secretary of Defense shall designate or appoint a White House Technology Liaison for the White House Communications Agency and the Secretary of Homeland Security shall designate or appoint a White House Technology Liaison for the United States Secret Service. Any entity that becomes a part of the Community after the issuance of this memorandum shall designate or appoint a White House Technology Liaison for that entity. The designation or appointment of a White House Technology Liaison is subject to the review of, and shall be made in consultation with, the President or his designee. The Chief Information Officer of the Office of Administration and the Chief Information Officer of the National Security Council, and their successors in function, are designated as White House Technology Liaisons for their respective components. In coordination with the Director, the White House Technology Liaisons shall ensure that the day-to-day operation of and long-term

18-F-1517//1622

strategy for information resources and information systems provided to the President, Vice President, and EOP are interoperable and effectively function as a single, modern, and high-quality enterprise that reduces duplication, inefficiency, and waste.

(d) The President or his designee shall retain the authority to specify the application of operating policies and procedures, including security measures, which are used in the construction, operation, and maintenance of any information resources or information system provided to the President, Vice President, and EOP.

(e) Presidential Information Technology Community entities shall:

(i) assist and provide information to the Deputy Chief of Staff for Operations and the Director, consistent with applicable law, as may be necessary to implement this memorandum; and

(ii) as soon as practicable after the issuance of this memorandum, enter into any memoranda of understanding as necessary to give effect to the provisions of this memorandum.

(f) As soon as practicable after the issuance of this memorandum, EOP components shall take all necessary steps, either individually or collectively, to ensure the proper creation, storage, and transmission of EOP information on any information systems and information resources provided to the President, Vice President, and EOP.

Sec. 5. Definitions. As used in this memorandum:

(a) "Information resources," "information systems," and "information technology" have the meanings assigned by section 3502 of title 44, United States Code.

(b) "Presidential Information Technology Community" means the entities that provide information resources and information systems to the President, Vice President, and EOP, including:

(i) the National Security Council;

(ii) the Office of Administration;

(iii) the United States Secret Service;

(iv) the White House Military Office; and

(v) the White House Communications Agency.

(c) "Executive Office of the President" means:

(i) each component of the EOP as is or may hereafter be established;

(ii) any successor in function to an EOP component that has been abolished and of which the function is retained in the EOP; and

(iii) the President's Commission on White House Fellowships, the President's Intelligence Advisory Board, the Residence of the Vice President, and such other entities as the President from time to time may determine.

Sec. 6. General Provisions. (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, entity, office, or the head thereof; or

18-F-1517//1623

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

Categories: Communications to Federal Agencies : White House Information Technology, Director, memorandum establishing; Executive Committee for Presidential Information Technology, memorandum establishing.

Subjects: White House Office : Assistants to the President :: White House Information Technology, Director; White House Office : Information Technology, Executive Committee for Presidential.

DCPD Number: DCPD201500185.

18-F-1517//1624

APPEAL,TYPE-D

U.S. District Court
District of Columbia (Washington, DC)
CIVIL DOCKET FOR CASE #: 1:17-cv-01320-CKK
Internal Use Only

ELECTRONIC PRIVACY INFORMATION CENTER v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY et al
Assigned to: Judge Colleen Kollar-Kotelly
Cases: 1:17-cv-01351-CKK
1:17-cv-01354-CKK
Cause: 05:702 Administrative Procedure Act

Date Filed: 07/03/2017
Jury Demand: None
Nature of Suit: 899 Administrative Procedure Act/Review or Appeal of Agency Decision
Jurisdiction: U.S. Government Defendant

Plaintiff

ELECTRONIC PRIVACY INFORMATION CENTER

represented by **Marc Rotenberg**
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140, ext 106
Fax: (202) 483-1248
Email: rotenberg@epic.org
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Alan Jay Butler
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140 ext 103
Fax: (202) 483-1248
Email: butler@epic.org
ATTORNEY TO BE NOTICED

Jeramie D. Scott
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140
Fax: (202) 483-1248
Email: jscott@epic.org
ATTORNEY TO BE NOTICED

V.

Defendant

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY

represented by **Carol Federighi**
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
(202) 514−1903
Email: carol.federighi@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
(202) 514−5302
Fax: (202) 616−8202
Email: Elizabeth.Shapiro@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
U.S. DEPARTMENT OF JUSTICE
P.O. Box 883
Washington, DC 20044
(202) 514−1944
Fax: (202) 616−8460
Email: joseph.borson@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
US DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
Suite 7000
Washington, DC 20001
(202) 353−4519
Email: kristina.wolfe@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

MICHAEL PENCE
In his official capacity as Chair of the Presidential Advisory Commission on Election Integrity

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

KRIS KOBACH
In his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

GENERAL SERVICES ADMINISTRATION

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

U.S. DEPARTMENT OF DEFENSE

represented by **Carol Federighi**
(See above for address)

LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

CHARLES G. HERNDON
in his official capacity as Director of White House Information Technology

represented by **Joseph Evan Borson**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

UNITED STATES DIGITAL SERVICE

represented by **Kristina Ann Wolfe**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY

represented by **Joseph Evan Borson**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Page	Docket Text
07/03/2017	1		COMPLAINT against EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY (Filing fee $ 400, receipt number 4616085803) filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Civil Cover Sheet)(td) (Entered: 07/03/2017)
07/03/2017			SUMMONS (8) Issued as to EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON

			ELECTION INTEGRITY, U.S. Attorney and U.S. Attorney General (td) (Entered: 07/03/2017)
07/03/2017	2		LCvR 7.1 CERTIFICATE OF DISCLOSURE of Corporate Affiliations and Financial Interests by ELECTRONIC PRIVACY INFORMATION CENTER (td) (Entered: 07/03/2017)
07/03/2017	3		MOTION for Temporary Restraining Order by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Exhibit, # 2 Text of Proposed Order)(td) (Entered: 07/03/2017)
07/03/2017			MINUTE ORDER: At approximately 4:50 P.M. EST, the Court held an on-the-record teleconference, attended by counsel for both parties, to set a briefing schedule on Plaintiff's 3 Emergency Motion for a Temporary Restraining Order. Defendants shall file their opposition to the motion by 4 P.M. EST on WEDNESDAY, JULY 5, 2017. Plaintiff shall file its reply by 9 A.M. EST on THURSDAY, JULY 6, 2017. Signed by Judge Colleen Kollar-Kotelly on 7/3/2017. (lcckk1) (Entered: 07/03/2017)
07/03/2017	4		ORDER Establishing Procedures for Cases Assigned to Judge Colleen Kollar-Kotelly. Signed by Judge Colleen Kollar-Kotelly on 07/03/2017. (DM) (Entered: 07/03/2017)
07/03/2017	5		NOTICE of Appearance by Elizabeth J. Shapiro on behalf of All Defendants (Shapiro, Elizabeth) (Entered: 07/03/2017)
07/03/2017			Minute Entry for proceedings held before Judge Colleen Kollar-Kotelly: Telephone Conference held on 7/3/2017. (Court Reporter Richard Ehrlich.) (dot) (Entered: 07/07/2017)
07/05/2017	6		NOTICE of Appearance by Carol Federighi on behalf of All Defendants (Federighi, Carol) (Entered: 07/05/2017)
07/05/2017	7		NOTICE of Appearance by Joseph Evan Borson on behalf of EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY (Borson, Joseph) (Entered: 07/05/2017)
07/05/2017	8		RESPONSE re 3 MOTION for Temporary Restraining Order filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Attachments: # 1 Declaration of Kris Kobach, # 2 Text of Proposed Order)(Federighi, Carol) (Entered: 07/05/2017)
07/05/2017	9		ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/5/2017. (lcckk1) (Entered: 07/05/2017)
07/06/2017	10		TRANSCRIPT OF SCHEDULING CONFERENCE before Judge Colleen Kollar-Kotelly held on July 3, 2017; Page Numbers: 1- 13. Date of Issuance: July 6, 2017. Court Reporter/Transcriber Richard D. Ehrlich, Telephone number 202-354-3269, Transcripts may be ordered by submitting the Transcript Order Form

			For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, CD or ASCII) may be purchased from the court reporter. **NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty−one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov. Redaction Request due 7/27/2017. Redacted Transcript Deadline set for 8/6/2017. Release of Transcript Restriction set for 10/4/2017.(Ehrlich, Richard) Modified date of hearing on 7/7/2017 (znmw). (Entered: 07/06/2017)
07/06/2017	11		RESPONSE TO ORDER OF THE COURT re 9 Order filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Attachments: # 1 Declaration of Kris W. Kobach)(Borson, Joseph) (Entered: 07/06/2017)
07/06/2017	12		NOTICE of Appearance by Alan Jay Butler on behalf of ELECTRONIC PRIVACY INFORMATION CENTER (Butler, Alan) (Entered: 07/06/2017)
07/06/2017	13		REPLY to opposition to motion re 3 MOTION for Temporary Restraining Order filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Addendum, # 2 Affirmation of Marc Rotenberg, # 3 Exhibits 1−11)(Butler, Alan) (Entered: 07/06/2017)
07/06/2017	14		ERRATA by ELECTRONIC PRIVACY INFORMATION CENTER 13 Reply to opposition to Motion filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Corrected Exhibit 11)(Butler, Alan) (Entered: 07/06/2017)
07/06/2017	15		ORDER. The Court hereby sets a hearing on Plaintiff's 3 Motion for a Temporary Restraining Order, to be held at 4:00 P.M. on July 7, 2017, in Courtroom 28A. Signed by Judge Colleen Kollar−Kotelly on 7/6/2017. (lcckk1) (Entered: 07/06/2017)
07/06/2017			Set/Reset Hearings: Motion Hearing set for 7/7/2017 at 4:00 PM in Courtroom 28A before Judge Colleen Kollar−Kotelly. (dot) (Entered: 07/07/2017)
07/07/2017	16		Unopposed MOTION for Leave to File *Surreply* by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY (Attachments: # 1 Exhibit Proposed Surreply, # 2 Text of Proposed Order)(Federighi, Carol) (Entered: 07/07/2017)
07/07/2017	17		

			RESPONSE TO ORDER OF THE COURT *Filing of Supplemental Brief* by ELECTRONIC PRIVACY INFORMATION CENTER re 15 Order (Butler, Alan) Modified event title on 7/10/2017 (znmw). (Entered: 07/07/2017)
07/07/2017	18		RESPONSE TO ORDER OF THE COURT re 15 Order *Defendants' Supplemental Brief on Informational Standing* filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Borson, Joseph) (Entered: 07/07/2017)
07/07/2017	19		Unopposed MOTION for Leave to File *Sur-surreply* by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Exhibit Proposed sur-surreply, # 2 Exhibit Exhibit to proposed sur-surreply, # 3 Text of Proposed Order)(Butler, Alan) (Entered: 07/07/2017)
07/07/2017	20		NOTICE *of Supplemental Exhibits* by ELECTRONIC PRIVACY INFORMATION CENTER re 15 Order (Attachments: # 1 Supplemental Exhibits)(Butler, Alan) (Entered: 07/07/2017)
07/07/2017			Minute Entry for proceedings held before Judge Colleen Kollar-Kotelly: Motion Hearing held on 7/7/2017 re 3 MOTION for Temporary Restraining Order filed by ELECTRONIC PRIVACY INFORMATION CENTER; and taken under advisement. (Court Reporter Richard Ehrlich.) (dot) (Entered: 07/07/2017)
07/07/2017	21		AMENDED COMPLAINT *pursuant to FRCP 15(a)(1)(A)* against ELECTRONIC PRIVACY INFORMATION CENTER filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Summons as to U.S. Department of Defense)(Butler, Alan) (Entered: 07/07/2017)
07/09/2017	22		TRANSCRIPT OF TEMPORARY RESTRAINING ORDER before Judge Colleen Kollar-Kotelly held on July 7, 2017; Page Numbers: 1 - 63. Date of Issuance:July 10, 2017. Court Reporter/Transcriber Richard D. Ehrlich, Telephone number (202) 354-3269, Transcripts may be ordered by submitting the Transcript Order Form For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased fro m the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi-page, condensed, CD or ASCII) may be purchased from the court reporter. **NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty-one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov. Redaction Request due 7/30/2017. Redacted Transcript Deadline set for 8/9/2017. Release of Transcript Restriction set for 10/7/2017.(Ehrlich, Richard) (Entered: 07/09/2017)

07/10/2017	23		ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/10/2017. (lcckk1) (Entered: 07/10/2017)
07/10/2017			Set/Reset Deadline: Supplemental briefing due by 4:00 PM on 7/10/2017. (tth) (Entered: 07/10/2017)
07/10/2017	24		RESPONSE TO ORDER OF THE COURT re 23 Order *Supplemental Brief re: DOD* filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Attachments: # 1 Declaration Third Kobach Decl.)(Borson, Joseph) (Entered: 07/10/2017)
07/10/2017	25		SUMMONS (1) Issued Electronically as to U.S. DEPARTMENT OF DEFENSE. (znmw) (Entered: 07/10/2017)
07/10/2017	26		ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/10/2017. (lcckk1) (Entered: 07/10/2017)
07/11/2017	27		RESPONSE TO ORDER OF THE COURT re 26 Order filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Butler, Alan) (Entered: 07/11/2017)
07/11/2017	28		NOTICE of Appearance by Jeramie D. Scott on behalf of ELECTRONIC PRIVACY INFORMATION CENTER (Scott, Jeramie) (Entered: 07/11/2017)
07/11/2017	29		MOTION for Leave to Appear Pro Hac Vice :Attorney Name- Caitriona Fitzgerald, :Firm- Electronic Privacy Information Center, :Address- 14 Tyler Street, Third Floor, Somerville, MA 02143. Phone No. - (617) 945-8409. Filing fee $ 100, receipt number 0090-5026343. Fee Status: Fee Paid. by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Declaration of Caitriona Fitzgerald, # 2 Text of Proposed Order)(Rotenberg, Marc) (Entered: 07/11/2017)
07/11/2017	30		MOTION for Leave to File *a Second Amended Complaint* by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Second Amended Complaint, # 2 Exhibit 5, # 3 Summons as to Charles C. Herndon, # 4 Summons as to U.S. Digital Service, # 5 Summons as to Executive Committee for Presidential Information Technology, # 6 Text of Proposed Order)(Butler, Alan) (Entered: 07/11/2017)
07/11/2017	31		ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/11/2017. (lcckk1) (Entered: 07/11/2017)
07/11/2017	32		RESPONSE re 30 MOTION for Leave to File *a Second Amended Complaint* filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, U.S. DEPARTMENT OF DEFENSE. (Federighi, Carol) (Entered: 07/11/2017)
07/11/2017			MINUTE ORDER: For good cause shown, and in light of Defendants' notice that they do not oppose this relief, ECF No. 32, Plaintiff's 30 Motion for Leave to File a Second Amended Complaint is GRANTED. Signed by Judge Colleen Kollar-Kotelly on 7/11/2017. (lcckk1) (Entered: 07/11/2017)

07/11/2017	33		SECOND AMENDED COMPLAINT against GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, U.S. DEPARTMENT OF DEFENSE, CHARLES G. HERNDON, UNITED STATES DIGITAL SERVICE, EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Exhibit 5)(znmw) (Entered: 07/12/2017)
07/12/2017	34		SUMMONS (3) Issued Electronically as to EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY, CHARLES G. HERNDON, UNITED STATES DIGITAL SERVICE. (znmw) (Entered: 07/12/2017)
07/13/2017	35		Amended MOTION for Temporary Restraining Order , MOTION for Preliminary Injunction by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Memorandum in Support, # 2 Exhibit List, # 3 Exhibit 1−20, # 4 Exhibit 21−30, # 5 Exhibit 31−40, # 6 Text of Proposed Order)(Butler, Alan) (Entered: 07/13/2017)
07/13/2017	36		ERRATA *Corrected Exhibits 21−30* by ELECTRONIC PRIVACY INFORMATION CENTER 35 Amended MOTION for Temporary Restraining Order MOTION for Preliminary Injunction filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Exhibit 21−30)(Butler, Alan) (Entered: 07/13/2017)
07/16/2017	37		NOTICE of Appearance by Kristina Ann Wolfe on behalf of All Defendants (Wolfe, Kristina) (Entered: 07/16/2017)
07/17/2017	38		RESPONSE re 35 Amended MOTION for Temporary Restraining Order MOTION for Preliminary Injunction filed by EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY, EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, CHARLES G. HERNDON, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE. (Attachments: # 1 Declaration, # 2 Text of Proposed Order)(Borson, Joseph) (Entered: 07/17/2017)
07/17/2017	39		REPLY to opposition to motion re 35 Amended MOTION for Temporary Restraining Order MOTION for Preliminary Injunction filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Declaration of Eleni Kyriakides)(Butler, Alan) (Entered: 07/17/2017)
07/18/2017			NOTICE OF ERROR re 39 Reply to opposition to Motion; emailed to butler@epic.org, cc'd 9 associated attorneys −− The PDF file you docketed contained errors: 1. FYI on future filings, the signature of the person filing and the one signing the document must match. (ztd,) (Entered: 07/18/2017)
07/24/2017	40	16	MEMORANDUM OPINION. Signed by Judge Colleen Kollar−Kotelly on 7/24/2017. (lcckk1) (Entered: 07/24/2017)
07/24/2017	41		ORDER. Plaintiff's 35 Motion for a Temporary Restraining Order and Preliminary Injunction is DENIED WITHOUT PREJUDICE. Signed by Judge Colleen Kollar−Kotelly on 7/24/2017. (lcckk1) (Entered: 07/24/2017)

07/25/2017	42	12	NOTICE OF APPEAL TO DC CIRCUIT COURT as to 41 Order on Motion for TRO, Order on Motion for Preliminary Injunction by ELECTRONIC PRIVACY INFORMATION CENTER. Filing fee $ 505, receipt number 0090−5047166. Fee Status: Fee Paid. Parties have been notified. (Attachments: # 1 Exhibit 1)(Rotenberg, Marc) (Entered: 07/25/2017)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*, Defendants.	Civ. Action No. 17-1320 (CKK)

PLAINTIFF'S NOTICE OF APPEAL

Notice is given this 25th day of July, 2017, that Plaintiff Electronic Privacy Information Center ("EPIC") hereby appeals to the United States Court of Appeals for the District of Columbia Circuit from the order of this Court denying Plaintiff's Motion for a Temporary Restraining Order and Preliminary Injunction, entered on the 24th day of July, 2017. Order, Ex. 1. EPIC brings this appeal pursuant to 28 U.S.C. § 1292 ("[T]he courts of appeals shall have jurisdiction of appeals from . . . [i]nterlocutory orders of the district courts . . . refusing . . . injunctions[.]").

EPIC seeks expedited review of the district court's Order, to which EPIC is entitled under 28 U.S.C. § 1657(a) ("[E]ach court of the United States shall expedite the consideration of any action . . . for temporary or preliminary injunctive relief."). EPIC is also entitled to expedited review because "good cause" exists for such treatment. *Id.* This case presents the type of extraordinary circumstances that justify expedited consideration. EPIC sought a TRO and preliminary injunction to block the Presidential Advisory Commission on Election Integrity ("the Commission") from collecting and aggregating state voter data from across the country (1) prior to completing and publishing a Privacy Impact Assessment as required by the E-Government Act

of 2002, 44 U.S.C. § 3501 note, and the Federal Advisory Committee Act, 5 U.S.C. app. 2; and (2) prior to the resolution of EPIC's constitutional privacy claims. The District Court denied EPIC's motion, concluding that "Defendants' collection of voter roll information does not currently involve *agency* action" as necessary for judicial review under the Administrative Procedure Act, 5 U.S.C. § 551 *et seq*. Memorandum Opinion 1 (emphasis added), ECF No. 40. Absent expedited review of the District Court's order by the Court of Appeals, the Commission will be allowed to systematically amass the sensitive, personal information of the nation's voters without establishing any procedures to protect voter privacy or the security and integrity of the data.

EPIC therefore respectfully requests that the Court of Appeals accord expedited treatment to this case.

/s/ Marc Rotenberg
MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel

CAITRIONA FITZGERALD*
EPIC Policy Director

JERAMIE D. SCOTT, D.C. Bar # 1025909
EPIC Domestic Surveillance Project Director

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Plaintiff EPIC

** Pro hac vice motion pending*

Dated: July 25, 2017

18-F-1517//1637

Exhibit 1

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 17-1320 (CKK)

ORDER
(July 24, 2017)

For the reasons stated in the accompanying Memorandum Opinion, Plaintiff's [35] Motion for a Temporary Restraining Order and Preliminary Injunction is **DENIED WITHOUT PREJUDICE**.

SO ORDERED.

Dated: July 24, 2017

/s/
COLLEEN KOLLAR-KOTELLY
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,
Plaintiff,
v.
PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,
Defendants.

Civil Action No. 17-1320 (CKK)

MEMORANDUM OPINION
(July 24, 2017)

This case arises from the establishment by Executive Order of the Presidential Advisory Commission on Election Integrity (the "Commission"), and a request by that Commission for each of the 50 states and the District of Columbia to provide it with certain publicly available voter roll information. Pending before the Court is Plaintiff's [35] Amended Motion for Temporary Restraining Order and Preliminary Injunction, which seeks injunctive relief prohibiting Defendants from "collecting voter roll data from states and state election officials" and directing Defendants to "delete and disgorge any voter roll data already collected or hereafter received." Proposed TRO, ECF No. 35-6, at 1-2.

Although substantial public attention has been focused on the Commission's request, the legal issues involved are highly technical. In addition to the Fifth Amendment of the Constitution, three federal laws are implicated: the Administrative Procedure Act, 5 U.S.C. § 551 *et seq.* ("APA"), the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 ("E-Government Act"), and the Federal Advisory Committee Act, codified at 5 U.S.C. app. 2 ("FACA"). All three are likely unfamiliar to the vast majority of Americans, and even seasoned legal practitioners are unlikely to have encountered the latter two.

Matters are further complicated by the doctrine of standing, a Constitutional prerequisite for this Court to consider the merits of this lawsuit.

Given the preliminary and emergency nature of the relief sought, the Court need not at this time decide conclusively whether Plaintiff is, or is not, ultimately entitled to relief on the merits. Rather, if Plaintiff has standing to bring this lawsuit, then relief may be granted if the Court finds that Plaintiff has a likelihood of succeeding on the merits, that it would suffer irreparable harm absent injunctive relief, and that other equitable factors—that is, questions of fairness, justice, and the public interest—warrant such relief.

The Court held a lengthy hearing on July 7, 2017, and has carefully reviewed the parties' voluminous submissions to the Court, the applicable law, and the record as a whole. Following the hearing, additional defendants were added to this lawsuit, and Plaintiff filed the pending, amended motion for injunctive relief, which has now been fully briefed. For the reasons detailed below, the Court finds that Plaintiff has standing to seek redress for the informational injuries that it has allegedly suffered as a result of Defendants declining to conduct and publish a Privacy Impact Assessment pursuant to the E-Government Act prior to initiating their collection of voter roll information. Plaintiff does not, however, have standing to pursue Constitutional or statutory claims on behalf of its advisory board members.

Although Plaintiff has won the standing battle, it proves to be a Pyrrhic victory. The E-Government Act does not itself provide for a cause of action, and consequently, Plaintiff must seek judicial review pursuant to the APA. However, the APA only applies to "agency action." Given the factual circumstances presently before the Court—which have changed substantially since this case was filed three weeks ago—Defendants' collection of voter

roll information does not currently involve agency action. Under the binding precedent of this circuit, entities in close proximity to the President, which do not wield "substantial independent authority," are not "agencies" for purposes of the APA. On this basis, neither the Commission or the Director of White House Information Technology—who is currently charged with collecting voter roll information on behalf of the Commission—are "agencies" for purposes of the APA, meaning the Court cannot presently exert judicial review over the collection process. To the extent the factual circumstances change, however—for example, if the *de jure* or *de facto* powers of the Commission expand beyond those of a purely advisory body—this determination may need to be revisited. Finally, the Court also finds that Plaintiff has not demonstrated an irreparable informational injury—given that the law does not presently entitle it to information—and that the equitable and public interest factors are in equipoise. These interests may very well be served by additional disclosure, but they would not be served by this Court, without a legal mandate, ordering the disclosure of information where no right to such information currently exists. Accordingly, upon consideration of the pleadings,[1] the relevant legal authorities, and the record as a whole, Plaintiff's [35] Motion for a Temporary Restraining Order and Preliminary Injunction is **DENIED WITHOUT PREJUDICE**.[2]

---

[1] The Court's consideration has focused on the following documents:

- Mem. in Supp. of Pl.'s Am. Mot. for a TRO and Prelim. Inj., ECF No. 35-1 ("Pls. Am. Mem.");
- Defs.' Mem. in Opp'n to Pl.'s Am. Mot. for a TRO and Prelim. Inj., ECF No. 38 ("Am. Opp'n Mem.");
- Reply in Supp. of Pl.'s Am. Mot. for a TRO and Prelim. Inj., ECF No. 39 ("Am. Reply Mem.").

[2] For the avoidance of doubt, the Court denies without prejudice both Plaintiff's motion for a temporary restraining order, and its motion for a preliminary injunction.

I. BACKGROUND

The Commission was established by Executive Order on May 11, 2017. Executive Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017) ("Exec. Order"). According to the Executive Order, the Commission's purpose is to "study the registration and voting processes used in Federal elections." *Id.* § 3. The Executive Order states that the Commission is "solely advisory," and that it shall disband 30 days after submitting a report to the President on three areas related to "voting processes" in federal elections. *Id.* §§ 3, 6. The Vice President is the chair of the Commission, and the President may appoint 15 additional members. From this group, the Vice President is permitted to appoint a Vice Chair of the Commission. The Vice President has named Kris W. Kobach, Secretary of State for Kansas, to serve as the Vice Chair. Decl. of Kris Kobach, ECF No. 8-1 ("Kobach Decl."), ¶ 1. Apart from the Vice President and the Vice Chair, there are presently ten other members of the Commission, including Commissioner Christy McCormick of the Election Assistance Commission (the "EAC"), who is currently the only federal agency official serving on the Commission, and a number of state election officials, both Democratic and Republican, and a Senior Legal Fellow of the Heritage Foundation. *Lawyers' Committee for Civil Rights Under the Law v. Presidential Advisory Commission on Election Integrity*, No. 17-cv-1354 (D.D.C. July 10, 2017), Decl. of Andrew J. Kossack, ECF No. 15-1 ("Kossack Decl."), ¶ 1; Second Decl. of Kris W. Kobach, ECF No. 11-1 ("Second Kobach Decl."), ¶ 1. According to Defendants, "McCormick is not serving in her official capacity as a member of the EAC." Second Kobach Decl. ¶ 2. The Executive Order also provides that the General Services Administration ("GSA"), a federal agency, will "provide the Commission with such administrative services, funds, facilities, staff, equipment, and other

support services as may be necessary to carry out its mission on a reimbursable basis," and that other federal agencies "shall endeavor to cooperate with the Commission." Exec. Order, § 7.

Following his appointment as Vice Chair, Mr. Kobach directed that identical letters "be sent to the secretaries of state or chief election officers of each of the fifty states and the District of Columbia." Kobach Decl. ¶ 4. In addition to soliciting the views of state officials on certain election matters by way of seven broad policy questions, each of the letters requests that state officials provide the Commission with the "publicly available voter roll data" of their respective states, "including, if publicly available under the laws of [their] state, the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information." Kobach Decl., Ex. 3 (June 28, 2017 Letter to the Honorable John Merrill, Secretary of State of Alabama). The letters sent by Mr. Kobach also indicate that "[a]ny documents that are submitted to the full Commission will . . . be made available to the public." *Id.* Defendants have represented that this statement applies only to "narrative responses" submitted by states to the Commission. *Id.* ¶ 5. "With respect to voter roll data, the Commission intends to de-identify any such data prior to any public release of documents. In other words, the voter rolls themselves will not be released to the public by the Commission." *Id.* The exact process by which de-identification and publication of voter roll data will occur has yet to be determined. Hr'g Tr. 36:20–37:8.

Each letter states that responses may be submitted electronically to an email address, ElectionIntegrityStaff@ovp.eop.gov, "or by utilizing the Safe Access File Exchange ('SAFE'), which is a secure FTP site the federal government uses for transferring large data files." Kobach Decl., Ex. 3. The SAFE website is accessible at https://safe.amrdec.army.mil/safe/ Welcome.aspx. Defendants have represented that it was their intention that "narrative responses" to the letters' broad policy questions should be sent via email, while voter roll information should be uploaded by using the SAFE system. *Id.* ¶ 5.

According to Defendants, the email address named in the letters "is a White House email address (in the Office of the Vice President) and subject to the security protecting all White House communications and networks." *Id.* Defendants, citing security concerns, declined to detail the extent to which other federal agencies are involved in the maintenance of the White House computer system. Hr'g Tr. 35:2-10. The SAFE system, however, is operated by the U.S. Army Aviation and Missile Research Development and Engineering Center, a component of the Department of Defense. Second Kobach Decl. ¶ 4; Hr'g Tr. 32:6–9. The SAFE system was "originally designed to provide Army Missile and Research, Development and Engineering Command (AMRDEC) employees and those doing business with AMRDEC an alternate way to send files." Safe Access File Exchange (Aug. 8, 2012), *available at* http://www.doncio.navy.mil/ContentView.aspx?id=4098 (last accessed July 20, 2017). The system allows "users to send up to 25 files securely to recipients within the .mil or .gov domains[,]" and may be used by anyone so long as the recipient has a .mil or .gov email address. After an individual uploads data via the SAFE system, the intended recipient receives an email message indicating that "they have been

18-F-1517//1645

given access to a file" on the system, and the message provides instructions for accessing the file. The message also indicates the date on which the file will be deleted. This "deletion date" is set by the originator of the file, and the default deletion date is seven days after the upload date, although a maximum of two weeks is permitted.

Defendants portrayed the SAFE system as a conduit for information. Once a state had uploaded voter roll information via the system, Defendants intended to download the data and store it on a White House computer system. Second Kobach Decl. ¶ 5. The exact details of how that would happen, and who would be involved, were unresolved at the time of the hearing. Hr'g Tr. 34:3–35:10; 35:23–36:9. Nonetheless, there is truth to Defendants' description. Files uploaded onto the system are not archived after their deletion date, and the system is meant to facilitate the transfer of files from one user to another, and is not intended for long-term data storage. As Defendants conceded, however, files uploaded onto the SAFE system are maintained for as many as fourteen days on a computer system operated by the Department of Defense. Hr'g Tr. 31:7–32:5; 36:1–9 (The Court: "You seem to be indicating that DOD's website would maintain it at least for the period of time until it got transferred, right?" Ms. Shapiro: "Yes. This conduit system would have it for – until it's downloaded. So from the time it's uploaded until the time it's downloaded for a maximum of two weeks and shorter if that's what's set by the states."). Defendants stated that as, of July 7, only the state of Arkansas had transmitted voter roll information to the Commission by uploading it to the SAFE system. Hr'g Tr. 40:10–18. According to Defendants, the Commission had not yet downloaded Arkansas' voter data; and as of the date of the hearing, the data continued to reside on the SAFE system. *Id.*

Shortly after the hearing, Plaintiff amended its complaint pursuant to Federal Rule

of Civil Procedure 15(a)(1)(A), and added the Department of Defense as a defendant. Am. Compl., ECF No. 21. The Court then permitted Defendants to file supplemental briefing with respect to any issues particular to the Department of Defense. Order, ECF No. 23. On July 10, Defendants submitted a Supplemental Brief, notifying the Court of certain factual developments since the July 7 hearing. First, Defendants represented that the Commission "no longer intends to use the DOD SAFE system to receive information from the states." Third Decl. of Kris W. Kobach, ECF No. 24-1 ("Third Kobach Decl."), ¶ 1. Instead, Defendants stated that the Director of White House Information Technology was working to "repurpos[e] an existing system that regularly accepts personally identifiable information through a secure, encrypted computer application," and that this new system was expected to be "fully functional by 6:00pm EDT [on July 10, 2017]." *Id.* Second, Defendants provided the Court with a follow-up communication sent to the states, directing election officials to "hold on submitting any data" until this Court resolved Plaintiff's motion for injunctive relief. *Id.*, Ex. A. In light of these developments, Plaintiff moved to further amend the complaint pursuant to Federal Rule of Civil Procedure 15(a)(2), to name as additional defendants the Director of White House Information Technology, the Executive Committee for Presidential Information Technology, and the United States Digital Service, which the Court granted. Pl.'s Mot. to Am. Compl., ECF No. 30; Order, ECF No. 31.

Given the "substantial changes in factual circumstances" since this action was filed, the Court directed Plaintiff to file an amended motion for injunctive relief. Order, ECF No. 31. Plaintiff filed the amended motion on July 13, seeking to enjoin Defendants from "collecting voter roll data from states and state election officials" and to require

18-F-1517//1647

Defendants to "disgorge any voter roll data already collected or hereafter received." Proposed Order, ECF No. 35-6, at 1–2. Defendants' response supplied additional information about how the voter roll data would be collected and stored by the "repurposed" White House computer system. *See* Decl. of Charles Christopher Herndon, ECF No. 38-1 ("Herndon Decl."), ¶¶ 3–6. According to Defendants, the new system requires state officials to request an access link, which then allows them to upload data to a "server within the domain electionintergrity.whitehouse.gov." *Id.* ¶ 4. Once the files have been uploaded, "[a]uthorized members of the Commission will be given access" with "dedicated laptops" to access the data through a secure White House network. *Id.* ¶ 4–5. Defendants represent that this process will only require the assistance of "a limited number of technical staff from the White House Office of Administration . . . ." *Id.* ¶ 6. Finally, Defendants represented that the voter roll data uploaded to the SAFE system by the state of Arkansas—the only voter roll information known to the Court that has been transferred in response to the Commission's request—"ha[d] been deleted without ever having been accessed by the Commission." *Id.* ¶ 7.

II. LEGAL STANDARD

Preliminary injunctive relief, whether in the form of temporary restraining order or a preliminary injunction, is "an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011) (quoting *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008)); *see also Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997) ("[A] preliminary injunction is an extraordinary and drastic remedy, one that should not be granted unless the movant, *by a clear showing*, carries the burden of persuasion." (emphasis in original;

quotation marks omitted)). A plaintiff seeking preliminary injunctive relief "must establish [1] that he is likely to succeed on the merits, [2] that he is likely to suffer irreparable harm in the absence of preliminary relief, [3] that the balance of equities tips in his favor, and [4] that an injunction is in the public interest." *Aamer v. Obama*, 742 F.3d 1023, 1038 (D.C. Cir. 2014) (quoting *Sherley*, 644 F.3d at 392 (quoting *Winter*, 555 U.S. at 20) (alteration in original; quotation marks omitted)). When seeking such relief, "'the movant has the burden to show that all four factors, taken together, weigh in favor of the injunction.'" *Abdullah v. Obama*, 753 F.3d 193, 197 (D.C. Cir. 2014) (quoting *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1292 (D.C. Cir. 2009)). "The four factors have typically been evaluated on a 'sliding scale.'" *Davis,* 571 F.3d at 1291 (citation omitted). Under this sliding-scale framework, "[i]f the movant makes an unusually strong showing on one of the factors, then it does not necessarily have to make as strong a showing on another factor." *Id.* at 1291–92.[3]

III. DISCUSSION

A. Article III Standing

As a threshold matter, the Court must determine whether Plaintiff has standing to

[3] The Court notes that it is not clear whether this circuit's sliding-scale approach to assessing the four preliminary injunction factors survives the Supreme Court's decision in *Winter*. *See Save Jobs USA v. U.S. Dep't of Homeland Sec.*, 105 F. Supp. 3d 108, 112 (D.D.C. 2015). Several judges on the United States Court of Appeals for the District of Columbia Circuit ("D.C. Circuit") have "read *Winter* at least to suggest if not to hold 'that a likelihood of success is an independent, free-standing requirement for a preliminary injunction.'" *Sherley*, 644 F.3d at 393 (quoting *Davis*, 571 F.3d at 1296 (concurring opinion)). However, the D.C. Circuit has yet to hold definitively that *Winter* has displaced the sliding-scale analysis. *See id.*; *see also Save Jobs USA*, 105 F. Supp. 3d at 112. In any event, this Court need not resolve the viability of the sliding-scale approach today, as it finds that Plaintiff has failed to show a likelihood of success on the merits and irreparable harm, and that the other preliminary injunction factors are in equipoise.

bring this lawsuit. Standing is an element of this Court's subject-matter jurisdiction under Article III of the Constitution, and requires, in essence, that a plaintiff have "a personal stake in the outcome of the controversy . . . ." *Warth v. Seldin*, 422 U.S. 490, 498 (1975). Consequently, a plaintiff cannot be a mere bystander or interested third-party, or a self-appointed representative of the public interest; he or she must show that defendant's conduct has affected them in a "personal and individual way." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). The familiar requirements of Article III standing are:

> (1) that the plaintiff have suffered an "injury in fact"—an invasion of a judicially cognizable interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) that there be a causal connection between the injury and the conduct complained of—the injury must be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court; and (3) that it be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Bennett v. Spear, 520 U.S. 154, 167 (1997) (citing *Lujan*, 504 U.S. at 560–61). The parties have briefed three theories of standing. Two are based on Plaintiff's own interests—for injuries to its informational interests and programmatic public interest activities—while the third is based on the interests of Plaintiff's advisory board members. This latter theory fails, but the first two succeed, for the reasons detailed below.

1. Associational Standing

An organization may sue to vindicate the interests of its members. To establish this type of "associational" standing, Plaintiff must show that "(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Ass'n of Flight Attendants-CWA, AFL-CIO v. U.S. Dep't of Transp.*, 564 F.3d 462, 464 (D.C. Cir. 2009) (internal

quotation marks omitted). Needless to say, Plaintiff must also show that it has "members" whose interests it is seeking to represent. To the extent Plaintiff does not have a formal membership, it may nonetheless assert organizational standing if "the organization is the functional equivalent of a traditional membership organization." *Fund Democracy, LLC v. S.E.C.*, 278 F.3d 21, 25 (D.C. Cir. 2002). For an organization to meet the test of functional equivalency, "(1) it must serve a specialized segment of the community; (2) it must represent individuals that have all the 'indicia of membership' including (i) electing the entity's leadership, (ii) serving in the entity, and (iii) financing the entity's activities; and (3) its fortunes must be tied closely to those of its constituency." *Washington Legal Found. v. Leavitt*, 477 F. Supp. 2d 202, 208 (D.D.C. 2007) (citing *Fund Democracy*, 278 F.3d at 25).

Plaintiff has submitted the declarations of nine advisory board members from six jurisdictions representing that the disclosure of their personal information—including "name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information"—will cause them immediate and irreparable harm. ECF No. 35-3, Exs. 7–15. The parties disagree on whether these advisory board members meet the test of functional equivalency. For one, Plaintiff's own website concedes that the organization "ha[s] no clients, no customers, and no shareholders . . . ." *See* About EPIC, http://epic.org/epic/about.html (last accessed July 20, 2017). Contrary to this assertion, however, Plaintiff has proffered testimony to the effect that advisory board members exert substantial influence over the affairs of the organization, including by influencing the matters in which the organization participates, and that advisory board members are

expected to contribute to the organization, either financially or by offering their time and expertise. Hr'g Tr. 16:1–18:19; *see also* Decl. of Marc Rotenberg, ECF No. 35-5, Ex. 38, ¶¶ 8–12. In the Court's view, however, the present record evidence is insufficient for Plaintiff to satisfy its burden with respect to associational standing. There is no evidence that members are *required* to finance the activities of the organization; that they have any role in electing the leadership of the organization; or that their fortunes, as opposed to their policy viewpoints, are "closely tied" to the organization. *See id.*; About EPIC, http://epic.org/epic/about.html (last accessed July 20, 2017) ("EPIC *works closely with* a distinguished advisory board, with expertise in law, technology and public policy. . . . EPIC is a 501(c)(3) nonprofit. We have no clients, no customers, and no shareholders. We need your support." (emphasis added)); *see also Elec. Privacy Info. Ctr. v. U.S. Dep't of Educ.*, 48 F. Supp. 3d 1, 22 (D.D.C. 2014) ("defendant raises serious questions about whether EPIC is an association made up of members that may avail itself of the associational standing doctrine").

Furthermore, even if the Court were to find that Plaintiff is functionally equivalent to a membership organization, the individual advisory board members who submitted declarations do not have standing to sue in their own capacities. First, these individuals are registered voters in states that have declined to comply with the Commission's request for voter roll information, and accordingly, they are not under imminent threat of either the statutory or Constitutional harms alleged by Plaintiff. *See* Am. Opp'n Mem., at 13. Second, apart from the alleged violations of the advisory board members' Constitutional privacy rights—the existence of which the Court assumes for purposes of its standing analysis, *see Parker v. D.C.*, 478 F.3d 370, 378 (D.C. Cir. 2007), *aff'd sub nom. D.C. v. Heller*, 554 U.S.

570 (2008)—Plaintiff has failed to proffer a theory of individual harm that is "actual or imminent, [and not merely] conjectural or hypothetical . . . [,]" *Bennett*, 520 U.S. at 167. Plaintiff contends that the disclosure of sensitive voter roll information would cause immeasurable harm that would be "impossible to contain . . . after the fact." Pl.'s Am. Mem., at 13. The organization also alleges that the information may be susceptible to appropriation for unspecified "deviant purposes." *Id.* (internal citations omitted). However, Defendants have represented that they are only collecting voter information that is already publicly available under the laws of the states where the information resides; that they have only requested this information and have not demanded it; and Defendants have clarified that such information, to the extent it is made public, will be de-identified. *See supra* at [•]. All of these representations were made to the Court in sworn declarations, and needless to say, the Court expects that Defendants shall strictly abide by them.

Under these factual circumstances, however, the only practical harm that Plaintiff's advisory board members would suffer, assuming their respective states decide to comply with the Commission's request in the future, is that their already publicly available information would be rendered more easily accessible by virtue of its consolidation on the computer systems that would ultimately receive this information on behalf of the Commission. It may be true, as Plaintiff contends, that there are restrictions on how "publicly available" voter information can be obtained in the ordinary course, such as application and notification procedures. Hr'g Tr. 8:2–21. But even granting the assumption that the Commission has or will receive information in a manner that bypasses these safeguards, the only way that such information would be rendered more accessible for nefarious purposes is if the Court further assumes that either the Commission systems are

more susceptible to compromise than those of the states, or that the de-identification process eventually used by Defendants will not sufficiently anonymize the information when it is publicized. Given the paucity of the record before the Court, this sequence of events is simply too attenuated to confer standing. At most, Plaintiff has shown that its members will suffer an increased *risk* of harm if their already publicly available information is collected by the Commission. But under the binding precedent of the Supreme Court, an increased risk of harm is insufficient to confer standing; rather, the harm must be "certainly impending." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013). Indeed, on this basis, two district courts in this circuit have concluded that even the disclosure of *confidential, identifiable* information is insufficient to confer standing until that information is or is about to be used by a third-party to the detriment of the individual whose information is disclosed. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 25 (D.D.C. 2014); *Welborn v. IRS*, 218 F. Supp. 3d 64, 77 (D.D.C. 2016). In sum, the mere increased risk of disclosure stemming from the collection and eventual, anonymized disclosure of already publicly available voter roll information is insufficient to confer standing upon Plaintiff's advisory board members. Consequently, for all of the foregoing reasons, Plaintiff has failed to show that it has associational standing to bring this lawsuit.[4]

[4] This obviates the need to engage in a merits analysis of Plaintiff's alleged Constitutional privacy right claims, which are based on the individual claims of its advisory board members. *See generally* Pl.'s Am. Mem., at 30. Nonetheless, even if the Court were to reach this issue, it would find that Plaintiff is unlikely to succeed on these claims because the D.C. Circuit has expressed "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information." *Am. Fed'n of Gov't Emps., AFL-CIO v. Dep't of Hous. & Urban Dev.*, 118 F.3d 786, 791 (D.C. Cir. 1997).

2. Informational Standing

In order to establish informational standing, Plaintiff must show that "(1) it has been deprived of information that, on its interpretation, a statute requires the government or a third party to disclose to it, and (2) it suffers, by being denied access to that information, the type of harm Congress sought to prevent by requiring disclosure." *Friends of Animals v. Jewell*, 828 F.3d 989, 992 (D.C. Cir. 2016). "[A] plaintiff seeking to demonstrate that it has informational standing generally 'need not allege any additional harm beyond the one Congress has identified.'" *Id.* (citing *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1544 (2016)). Plaintiff has brought suit under the APA, for the failure of one or more federal agencies to comply with Section 208 of the E-Government Act. That provision mandates that before "initiating a new collection of information," an agency must "conduct a privacy impact assessment," "ensure the review of the privacy impact assessment by the Chief Information Officer," and "if practicable, after completion of the review . . . , make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." E-Government Act, § 208(b). An enumerated purpose of the E-Government Act is "[t]o make the Federal Government more transparent and accountable." *Id.* § 2(b)(9).

Plaintiff satisfies both prongs of the test for informational standing. First, it has espoused a view of the law that entitles it to information. Namely, Plaintiff contends that Defendants are engaged in a new collection of information, and that a cause of action is available under the APA to force their compliance with the E-Government Act and to require the disclosure of a Privacy Impact Assessment. Second, Plaintiff contends that it has suffered the very injuries meant to be prevented by the disclosure of information

pursuant to the E-Government Act—lack of transparency and the resulting lack of opportunity to hold the federal government to account. This injury is particular to Plaintiff, given that it is an organization that was "established . . . to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age." About EPIC, https://www.epic.org/epic /about.html (last accessed July 20, 2017). Plaintiff, moreover, engages in government outreach by "speaking before Congress and judicial organizations about emerging privacy and civil liberties issues[,]" *id.*, and uses information it obtains from the government to carry out its mission to educate the public regarding privacy issues, Hr'g Tr. 20:12–23.

Defendants have contested Plaintiff's informational standing, citing principally to the D.C. Circuit's analysis in *Friends of Animals*. *See* Am. Opp'n Mem., at 14–20. There, the court held that plaintiff, an environmental organization, did not have informational standing under a statute that required the Department of the Interior ("DOI"), *first*, to make certain findings regarding whether the listing of a species as endangered is warranted within 12 months of determining that a petition seeking that relief "presents substantial scientific or commercial information," and *second*, after making that finding, to publish certain information in the Federal Register, including under some circumstances, a proposed regulation, or an "evaluation of the reasons and data on which the finding is based." *Friends of Animals*, 828 F.3d at 990–91 (internal quotation marks omitted) (citing 16 U.S.C. § 1533(b)(3)(B)). For example, part of the statute in *Friends of Animals* required that:

> (B) Within 12 months after receiving a petition that is found under subparagraph (A) to present substantial information indicating that the petitioned action may be warranted, the Secretary shall make one of the following findings: . . .
>
> > (ii) The petitioned action is warranted, in which case the Secretary shall promptly publish in the Federal Register a general notice and the complete text of a proposed regulation to implement such action in accordance with paragraph (5).

16 U.S.C. § 1533(b)(3)(B)(ii). At the time plaintiff brought suit, the 12-month period had elapsed, but the DOI had yet to make the necessary findings, and consequently had not published any information in the Federal Register. In assessing plaintiff's informational standing, the D.C. Circuit focused principally on the structure of the statute that allegedly conferred on plaintiff a right to information from the federal government. *Friends of Animals*, 828 F.3d at 993. Solely on that basis, the court determined that plaintiff was not entitled to information because a right to information (e.g., a proposed regulation under subsection (B)(ii) or an evaluation under subsection (B)(iii)) arose only *after* the DOI had made one of the three findings envisioned by the statute. True, the DOI had failed to make the requisite finding within 12 months. But given the statutorily prescribed sequence of events, plaintiff's challenge was in effect to the DOI's failure to make such a finding, rather than to its failure to disclose information, given that the obligation to disclose information only arose after a finding had been made. As such, the D.C. Circuit concluded that plaintiff lacked informational standing.

The statutory structure here, however, is quite different. The relevant portion of Section 208 provides the following:

> (b) PRIVACY IMPACT ASSESSMENTS.—
> (1) RESPONSIBILITIES OF AGENCIES.
> (A) IN GENERAL.—An agency shall take actions described under subparagraph (B) before
> (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
> (ii) initiating a new collection of information that—
> (I) will be collected, maintained, or disseminated using information technology; and
> (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.
> (B) AGENCY ACTIVITIES.—To the extent required under subparagraph (A), each agency shall—
> (i) conduct a privacy impact assessment;
> (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and
> (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

E-Government Act, § 208(b). As this text makes clear, the statutorily prescribed sequence of events here is reversed from the sequence at issue in *Friends of Animals*. There, the DOI was required to disclose information only *after* it had made one of three "warranted" findings; it had not made any finding, and accordingly, was not obligated to disclose any information. Here, the statute mandates that an "agency *shall* take actions described under subparagraph (B) *before* . . . initiating a new collection of information . . . ." *Id.* (emphasis added). Subparagraph (B) in turn requires the agency to conduct a Privacy Impact Assessment, to have it reviewed by the Chief Information Officer or his equivalent, and to publish the assessment, if practicable. The statute, given its construction, requires all three of these events, including the public disclosure of the assessment, to occur *before* the

agency initiates a new collection of information. Assuming that the other facets of Plaintiff's interpretation of the law are correct—namely, that Defendants are engaged in a new collection of information subject to the E-Government Act, that judicial review is available under the APA, and that disclosure of a privacy assessment is "practicable"—then Plaintiff is presently entitled to information pursuant to the E-Government Act, because the disclosure of information was already supposed to have occurred; that is, a Privacy Impact Assessment should have been made publicly available before Defendants systematically began collecting voter roll information. Accordingly, unlike in *Friends of Animals*, a review of the statutory text at issue in this litigation indicates that, under Plaintiff's interpretation of the law, Defendants have already incurred an obligation to disclose information.

Defendants make three further challenges to Plaintiff's informational standing, none of which are meritorious. First, Defendants contend that Plaintiff lacks standing because its informational injury is merely a "generalized grievance," and therefore insufficient to confer standing. Am. Opp'n Mem., at 15 (citing *Judicial Watch, Inc. v. FEC*, 180 F.3d 277, 278 (D.C. Cir. 1999)). Plainly, the E-Government Act entitles the public generally to the disclosure of Privacy Impact Assessments, but that does not mean that the informational injury in this case is not particular to Plaintiff. As already noted, Plaintiff is a public-interest organization that focuses on privacy issues, and uses information gleaned from the government to educate the public regarding privacy, and to petition the government regarding privacy law. *See supra* at [•]. Accordingly, the informational harm in this case, as it relates to Plaintiff, is "concrete and particularized." Moreover, the reality of statutes that confer informational standing is that they are often not targeted at a

particular class of individuals, but rather provide for disclosure to the public writ large. *See, e.g.*, *Friends of Animals*, 824 F.3d at 1041 (finding that public interest environmental organization had standing under statutory provision that required the Department of the Interior to publish certain information in the Federal Register). Even putting aside the particularized nature of the informational harm alleged in this action, however, the fact that a substantial percentage of the public is subject to the same harm does not automatically render that harm inactionable. As the Supreme Court observed in *Akins*: "Often the fact that an interest is abstract and the fact that it is widely shared go hand in hand. But their association is not invariable, and where a harm is concrete, though widely shared, the Court has found 'injury in fact.'" *FEC v. Akins*, 524 U.S. 11, 24 (1998). The Court went on to hold, in language that is particularly apt under the circumstances, that "the informational injury at issue . . . , directly related to voting, the most basic of political rights, is sufficiently concrete and specific . . . ." *Id.* at 24–25.

Defendants next focus on the fact that the information sought does not yet exist in the format in which it needs to be disclosed (i.e., as a Privacy Impact Assessment). Am. Opp'n Mem., at 17. In this vein, they claim that *Friends of Animals* stands for the proposition that the government cannot be required to create information. The Court disagrees with this interpretation of *Friends of Animals*, and moreover, Defendants' view of the law is not evident in the controlling Supreme Court and D.C. Circuit precedents. As already detailed, the court in *Friends of Animals* looked solely to the statutory text to determine whether an obligation to disclose had been incurred. No significance was placed by the D.C. Circuit on the fact that, if there were such an obligation, the federal government would potentially be required to "create" the material to be disclosed (in that case, either a

proposed regulation, or an evaluative report). Furthermore, *Friends of Animals* cited two cases, one by the D.C. Circuit and the other by the Supreme Court, as standing for the proposition that plaintiffs have informational standing to sue under "statutory provisions that guarantee[] a right to receive information *in a particular form*." *Friends of Animals*, 828 F.3d at 994 (emphasis added; citing *Zivotofsky ex rel. Ari Z. v. Sec'y of State*, 444 F.3d 614, 615–19 (D.C. Cir. 2006), and *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373–75 (1982)). Furthermore, in *Public Citizen*, the Supreme Court found that plaintiff had informational standing to sue under FACA, and thereby seek the disclosure of an advisory committee charter and other materials which FACA requires advisory committees to create and make public. Presumably those materials did not exist, given defendants' position that the committee was not subject to FACA, and in any event, the Court made no distinction on this basis. *Pub. Citizen v. U.S. Dep't of Justice*, 491 U.S. 440, 447 (1989). And in *Akins*, the information sought was not in defendants' possession, as the entire lawsuit was premised on requiring defendant to take enforcement action to obtain that information. 524 U.S. at 26. Ultimately, the distinction between information that already exists, and information that needs to be "created," if not specious, strikes the Court as an unworkable legal standard. Information does not exist is some ideal form. When the government discloses information, it must always first be culled, organized, redacted, reviewed, and produced. Sometimes the product of that process, as under the Freedom of Information Act, is a production of documents, perhaps with an attendant privilege log. *See, e.g., Judicial Watch, Inc. v. Food & Drug Admin.*, 449 F.3d 141, 146 (D.C. Cir. 2006) (explaining the purpose of a *Vaughn* index). Here, Congress has mandated that disclosure take the form of a Privacy Impact Assessment, and that is what Plaintiff has standing to

seek, regardless of whether an agency is ultimately required to create the report.

Lastly, Defendants contend that Plaintiff lacks informational standing because Section 208 only requires the publication of a Privacy Impact Statement if doing so is "practicable." Am. Opp'n Mem., at 17 n.2. As an initial matter, Defendants have at no point asserted that it would be impracticable to create and publish a Privacy Impact Assessment; rather, they have rested principally on their contention that they are not required to create or disclose one because Plaintiff either lacks standing, or because the E-Government Act and APA only apply to federal agencies, which are not implicated by the collection of voter roll information. Accordingly, whatever limits the word "practicable" imposes on the disclosure obligations of Section 208, they are not applicable in this case, and therefore do not affect Plaintiff's standing to bring this lawsuit. As a more general matter, however, the Court disagrees with Defendants' view that merely because a right to information is in some way qualified, a plaintiff lacks informational standing to seek vindication of that right. For this proposition, Defendants again cite *Friends of Animals*, contending that the D.C. Circuit held that "informational standing only exists if [the] statute 'guaranteed a right to receive information in a particular form . . . .'" *Id.* (citing *Friends of Animals*, 828 F.3d at 994). That is not what the D.C. Circuit held; rather that language was merely used to describe two other cases, *Haven* and *Zivotofsky*, in which the Supreme Court and D.C. Circuit determined that plaintiffs had informational standing. *See supra* at [•]. One only need to look toward the Freedom of Information Act, under which litigants undoubtedly have informational standing despite the fact that the Act in no way provides an unqualified right to information, given its numerous statutory exemptions. *See Zivotofsky*, 444 F.3d at 618. Moreover, the available guidance indicates that the qualifier "practicable" was meant

to function similarly to the exemptions under the Freedom of Information Act, and is therefore not purely discretionary. *See* M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003) ("Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment. *Such information shall be protected and handled consistent with the Freedom of Information Act* . . . ." (footnote omitted; emphasis added)). Accordingly, for all of the foregoing reasons, the Court concludes that Plaintiff has satisfied its burden at this stage regarding its informational standing to seek the disclosure of a Privacy Impact Assessment pursuant to Section 208 of the E-Government Act.

Moreover, because the Court assumes the merits of Plaintiff's claims for standing purposes, the Court also finds that Plaintiff has informational standing with respect to its FACA claim, which likewise seeks the disclosure of a Privacy Impact Assessment. *Judicial Watch, Inc. v. U.S. Dep't of Commerce*, 583 F.3d 871, 873 (D.C. Cir. 2009) ("Here the injury requirement is obviously met. In the context of a FACA claim, an agency's refusal to disclose information that the act requires be revealed constitutes a sufficient injury.)

3. Organizational Standing Under PETA

For similar reasons to those enumerated above with respect to informational standing, the Court also finds that Plaintiff has organizational standing under *PETA v. USDA*, 797 F.3d 1087 (D.C. Cir. 2015). In this circuit, an organization may establish standing if it has "suffered a concrete and demonstrable injury to its activities, mindful that,

18-F-1517//1663

under our precedent, a mere setback to . . . abstract social interests is not sufficient." *Id.* at 1093 (internal quotation marks and alterations omitted) (citing *Am. Legal Found. v. FCC*, 808 F.2d 84, 92 (D.C. Cir. 1987) ("The organization must allege that discrete programmatic concerns are being directly and adversely affected by the defendant's actions."). "Making this determination is a two-part inquiry—we ask, first, whether the agency's action or omission to act injured the organization's interest and, second, whether the organization used its resources to counteract that harm." *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 919 (D.C. Cir. 2015) (internal quotation marks and alterations omitted). In *PETA*, the D.C. Circuit found that an animal rights organization had suffered a "denial of access to bird-related . . . information including, in particular, investigatory information, and a means by which to seek redress for bird abuse . . . ." *PETA*, 797 F.3d at 1095. This constituted a "cognizable injury sufficient to support standing" because the agency's failure to comply with applicable regulations had impaired PETA's ability to bring "violations to the attention of the agency charged with preventing avian cruelty and [to] continue to educate the public." *Id.*

Under the circumstances of this case, Plaintiff satisfies the requirements for organizational standing under *PETA*. Plaintiff has a long-standing mission to educate the public regarding privacy rights, and engages in this process by obtaining information from the government. Pl.'s Reply Mem. at 17 ("EPIC's mission includes, in particular, educating the public about the government's record on voter privacy and promoting safeguards for personal voter data."). Indeed, Plaintiff has filed Freedom of Information Act requests in this jurisdiction seeking the disclosure of the same type of information, Privacy Impact Assessments, that it claims has been denied in this case. *See, e.g., Elec. Privacy Info. Ctr.*

v. DEA, 208 F. Supp. 3d 108, 110 (D.D.C. 2016). Furthermore, Plaintiff's programmatic activities—educating the public regarding privacy matters—have been impaired by Defendants' alleged failure to comply with Section 208 of the E-Government Act, since those activities routinely rely upon access to information from the federal government. *See* Hr'g Tr. at 20:8–16. This injury has required Plaintiff to expend resources by, at minimum, seeking records from the Commission and other federal entities concerning the collection of voter data. *See* Decl. of Eleni Kyriakides, ECF No. 39-1, ¶ 6. Accordingly, Plaintiff has organizational standing under the two-part test sanctioned by the D.C. Circuit in *PETA*.

B. Likelihood of Success on the Merits

Having assured itself of Plaintiff's standing to bring this lawsuit, the Court turns to assess the familiar factors for determining whether a litigant is entitled to preliminary injunctive relief; in this case, a temporary restraining order and preliminary injunction. The first, and perhaps most important factor, is Plaintiff's likelihood of success on the merits.

The E-Government Act does not provide for a private cause of action, and accordingly, Plaintiff has sought judicial review pursuant to Section 702 of the APA. *See Greenspan v. Admin. Office of the United States Courts*, No. 14CV2396 JTM, 2014 WL 6847460, at *8 (N.D. Cal. Dec. 4, 2014). Section 704 of the APA, in turn, limits judicial review to "final agency action for which there is no other adequate remedy . . . ." As relevant here, the reviewing court may "compel agency action unlawfully withheld or unreasonably delayed." 5 U.S.C. § 706(1). The parties principally disagree over whether any "agency" is implicated in this case such that there could be an "agency action" subject to this Court's review. *See* Pl.'s Am. Mem., at 19–30; Am. Opp'n Mem., at 20–33.

"Agency" is broadly defined by the APA to include "each authority of the

Government of the United States, whether or not it is within or subject to review by another agency . . . ." 5 U.S.C. § 551(1). The statute goes on to exclude certain components of the federal government, including Congress and the federal courts, but does not by its express terms exclude the President, or the Executive Office of the President ("EOP"). *Id.* Nonetheless, the Supreme Court has concluded that the President is exempted from the reach of the APA, *Franklin v. Massachusetts*, 505 U.S. 788, 800–01 (1992), and the D.C. Circuit has established a test for determining whether certain bodies within the Executive Office of the President are sufficiently close to the President as to also be excluded from APA review, *see Armstrong v. Exec. Office of the President*, 90 F.3d 553, 558 (D.C. Cir. 1996) (citing *Meyer v. Bush*, 981 F.2d 1288 (D.C. Cir. 1993)). In determining whether the Commission is an "agency," or merely an advisory body to the President that is exempted from APA review, relevant considerations include "whether the entity exercises substantial independent authority," "whether the entity's sole function is to advise and assist the President," "how close operationally the group is to the President," "whether it has a self-contained structure," and "the nature of its delegated authority." *Citizens for Responsibility & Ethics in Washington v. Office of Admin.*, 566 F.3d 219, 222 (D.C. Cir. 2009) ("*CREW*") (internal quotation marks omitted). The most important consideration appears to be whether the "entity in question wielded substantial authority independently of the President." *Id.*

The record presently before the Court is insufficient to demonstrate that the Commission is an "agency" for purposes of the APA. First, the Executive Order indicates that the Commission is purely advisory in nature, and that it shall disband shortly after it delivers a report to the President. No independent authority is imbued upon the

Commission by the Executive Order, and there is no evidence that it has exercised any independent authority that is unrelated to its advisory mission. Defendants' request for information is just that—a request—and there is no evidence that they have sought to turn the request into a demand, or to enforce the request by any means. Furthermore, the request for voter roll information, according to Defendants, is ancillary to the Commission's stated purpose of producing an advisory report for the President regarding voting processes in federal elections. The Executive Order does provide that other federal agencies "shall endeavor to cooperate with the Commission," and that the GSA shall "provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission." Exec. Order § 7(a). Nonetheless, Defendants have represented that the GSA's role is currently expected to be limited to specific "administrative support like arranging travel for the members" of the Commission, and that no other federal agencies are "cooperating" with the Commission. Hr'g Tr. at 27:25–28:6; 30:10–13. Finally, although Commissioner Christy McCormick of the Election Assistance Commission is a member of the Commission, there is currently no record evidence that she was substantially involved in the decision to collect voter information, or that her involvement in some fashion implicated the Election Assistance Commission, which is a federal agency. Hr'g Tr. 28:24–30:4; *cf. Judicial Watch, Inc. v. Nat'l Energy Policy Dev. Grp.*, 219 F. Supp. 2d 20, 39–40 (D.D.C. 2002) (citing *Ryan v. Dep't of Justice*, 617 F.2d 781 (D.C. Cir. 1980)).

This would have ended the inquiry, but for the revelation during the course of these proceedings that the SAFE system, which the Commission had intended for states to use to transmit voter roll information, is operated by a component of the Department of

18-F-1517//1667

Defense. Moreover, the only voter roll information transferred to date resided on the SAFE system, and consequently was stored on a computer system operated by the Department of Defense. Given these factual developments, the Department of Defense—a federal agency—was added as a defendant to this lawsuit. *See* Am. Compl., ECF No. 21, ¶¶ 37–42. Shortly after that occurred, however, Defendants changed gears, and represented that "[i]n order not to impact the ability of other customers to use the [SAFE] site, the Commission has decided to use alternative means for transmitting the requested data." ECF No. 24, at 1. In lieu of the SAFE system, Defendants had the Director of White House Information Technology ("DWHIT") repurpose "an existing system that regularly accepts personally identifiable information through a secure, encrypted computer application within the White House Information Technology enterprise." *Id.* Furthermore, Defendants have represented that the data received from the State of Arkansas via the SAFE system has been deleted, "without ever having been accessed by the Commission." Herndon Decl. ¶ 7. Accordingly, while the legal dispute with respect to the use of the SAFE system by Defendants to collect at least some voter roll information may not be moot—data was in fact collected before a Privacy Impact Assessment was conducted pursuant to the E-Government Act—that potential legal violation does not appear to be a basis for the prospective injunctive relief sought by Plaintiff's amended motion for injunctive relief; namely, the prevention of the further collection of voter roll information by the Commission. In any event, Plaintiff has not pursued the conduct of the Department of Defense as a basis for injunctive relief.

Given the change of factual circumstances, the question now becomes whether any of the entities that will be involved in administering the "repurposed" White House system

are "agencies" for purposes of APA review. One candidate is the DWHIT. According to the Presidential Memorandum establishing this position, the "Director of White House Information Technology, on behalf of the President, shall have the primary authority to establish and coordinate the necessary policies and procedures for operating and maintaining the information resources and information systems provided to the President, Vice President, and the EOP." Mem. on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology ("DWHIT Mem."), § 1, *available at* https://www.gpo.gov/fdsys/pkg/DCPD-201500185/pdf/DCPD-201500185.pdf (last accessed July 16, 2017). The DWHIT is part of the White House Office, *id.* § 2(a)(ii), a component of the EOP "whose members assist the President with those tasks incidental to the office." *Alexander v. F.B.I.*, 691 F. Supp. 2d 182, 186 (D.D.C. 2010), *aff'd*, 456 F. App'x 1 (D.C. Cir. 2011); *see also* Herndon Decl. ¶ 1. According to the Memorandum, the DWHIT "shall ensure the effective use of information resources and information systems provided to the President, Vice President, and EOP in order to improve mission performance, and shall have the appropriate authority to promulgate all necessary procedures and rules governing these resources and systems." DWHIT Mem., § 2(c). The DWHIT is also responsible for providing "policy coordination and guidance" for a group of other entities that provide information technology services to the President, Vice President, and the EOP, known as the "Presidential Information Technology Community." *Id.* § 2(a), (c). Furthermore, the DWHIT may "advise and confer with appropriate executive departments and agencies, individuals, and other entities as necessary to perform the Director's duties under this memorandum." *Id.* § 2(d).

Taken as a whole, the responsibilities of the DWHIT based on the present record

amount to providing operational and administrative support services for information technology used by the President, Vice President, and close staff. Furthermore, to the extent there is coordination with other federal agencies, the purpose of that coordination is likewise to ensure the sufficiency and quality of information services provided to the President, Vice President, and their close staff. Given the nature of the DWHIT's responsibilities and its proximity to the President and Vice President, it is not an agency for the reasons specified by the D.C. Circuit in *CREW* with respect to the Office of Administration ("OA"). In that case, the D.C. Circuit held that the OA was not an "agency" under FOIA[5] because "nothing in the record indicate[d] that OA performs or is authorized to perform tasks other than operational and administrative support for the President and his staff . . . ." *CREW*, 566 F.3d at 224. Relying on its prior holding in *Sweetland*, the court held that where an entity within the EOP, like the DWHIT, provides to the President and his staff "only operational and administrative support . . . it lacks the substantial

[5] Plaintiff argues that *CREW* and similar cases by the D.C. Circuit interpreting whether an entity is an agency for purposes of FOIA are not applicable to determining whether an entity is an agency for purposes of the APA. *See* Pl.'s Reply Mem. at 2. The Court disagrees. The D.C. Circuit established the "substantial independent authority" test in *Soucie*, a case that was brought under FOIA, but at a time when the definition of "agency" for FOIA purposes mirrored the APA definition. In that case, the D.C. Circuit held that "the APA apparently confers agency status on any administrative unit with *substantial independent authority* in the exercise of specific functions." *Soucie v. David*, 448 F.2d 1067, 1073 (D.C. Cir. 1971) (emphasis added); *Meyer*, 981 F.2d at 1292 n.1 ("[b]efore the 1974 Amendments, FOIA simply had adopted the APA's definition of agency"); *see also Dong v. Smithsonian Inst.*, 125 F.3d 877, 881 (D.C. Cir. 1997) ("[o]ur cases have followed the same approach, requiring that an entity exercise substantial independent authority before it can be considered an agency for § 551(1) purposes"—that is, the section that defines the term "agency" for purposes of the APA). The *CREW* court applied the "substantial independent authority" test, and the Court sees no basis to hold that the reasoning of *CREW* is not dispositive of DWHIT's agency status in this matter.

independent authority we have required to find an agency covered by FOIA . . . ." *Id.* at 223 (citing *Sweetland v. Walters*, 60 F.3d 852, 854 (D.C. Cir. 1995)). This conclusion was unchanged by the fact that the OA, like the DWHIT here, provides support for other federal agencies to the extent they "work at the White House complex in support of the President and his staff." *Id.* at 224. Put differently, the fact that the DWHIT coordinates the information technology support provided by other agencies for the President, Vice President, and their close staff, does not change the ultimate conclusion that the DWHIT is not "authorized to perform tasks other than operational and administrative support for the President and his staff," which means that the DWHIT "lacks substantial independent authority and is therefore not an agency . . . ." *Id.* However, to the extent that DWHIT's responsibilities expand either formally or organically, as a result of its newfound responsibilities in assisting the Commission, this determination may need to be revisited in the factual context of this case.

The other candidates for "agency action" proposed by Plaintiff fare no better. The Executive Committee for Presidential Information Technology and the U.S. Digital Service, even if they were agencies, "will have no role in th[e] data collection process." Herndon Decl. ¶ 6. According to Defendants, apart from the DWHIT, the only individuals who will be involved in the collection of voter roll information are "a limited number of . . . technical staff from the White House Office of Administration." *Id.* Finally, Plaintiff contends that the entire EOP is a "parent agency," and that as a result, the activities of its components, including those of the DWHIT and the Commission, are subject to APA review. However, this view of the EOP has been expressly rejected by the D.C. Circuit and is at odds with the practical reality that the D.C. Circuit has consistently analyzed the

18-F-1517//1671

agency status of EOP components on a component-by-component basis. *United States v. Espy*, 145 F.3d 1369, 1373 (D.C. Cir. 1998) ("it has never been thought that the whole Executive Office of the President could be considered a discrete agency under FOIA"). Accordingly, at the present time and based on the record before the Court, it appears that there is no "agency," as that term is understood for purposes of the APA, that is involved in the collection of voter roll information on behalf of the Commission. Because there is no apparent agency involvement at this time, the Court concludes that APA review is presently unavailable in connection with the collection of voter roll information by the Commission.

The last remaining avenue of potential legal redress is pursuant to FACA. Plaintiff relies on Section 10(b) of FACA as a means to seek the disclosure of a Privacy Impact Assessment, as required under certain circumstances by the E-Government Act. *See* Am. Compl, ECF No. 33, ¶¶ 73–74. That section provides that an advisory committee subject to FACA must make publicly available, unless an exception applies under FOIA, "the records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by [the] advisory committee . . . ." 5 U.S.C. app. 2 § 10(b). The flaw with this final approach, however, is that FACA itself does not require Defendants to produce a Privacy Impact Assessment; only the E-Government Act so mandates, and as concluded above, the Court is not presently empowered to exert judicial review pursuant to the APA with respect to Plaintiff's claims under the E-Government Act, nor can judicial review be sought pursuant to the E-Government Act itself, since it does not provide for a private cause of action. Consequently, for all of the foregoing reasons, none of Plaintiff's avenues of potential legal redress appear

to be viable at the present time, and Plaintiff has not demonstrated a likelihood of success on the merits.

C. Irreparable Harm, Balance of the Equities, and the Public Interest

Given that Plaintiff is essentially limited to pursuing an informational injury, many of its theories of irreparable harm, predicated as they are on injuries to the private interests of its advisory board members, have been rendered moot. *See* Pl.'s Am. Mem., at 34–40. Nonetheless, the non-disclosure of information to which a plaintiff is entitled, under certain circumstances itself constitutes an irreparable harm; specifically, where the information is highly relevant to an ongoing and highly public matter. *See, e.g.*, *Elec. Privacy Info. Ctr. v. Dep't of Justice*, 416 F. Supp. 2d 30, 41 (D.D.C. 2006) ("EPIC will also be precluded, absent a preliminary injunction, from obtaining in a timely fashion information vital to the current and ongoing debate surrounding the legality of the Administration's warrantless surveillance program"); *see also Washington Post v. Dep't of Homeland Sec.*, 459 F. Supp. 2d 61, 75 (D.D.C. 2006) ("Because the urgency with which the plaintiff makes its FOIA request is predicated on a matter of current national debate, due to the impending election, a likelihood for irreparable harm exists if the plaintiff's FOIA request does not receive expedited treatment."). Indeed, the D.C. Circuit has held that "stale information is of little value . . . [,]" *Payne Enters, Inc. v. United States*, 837 F.2d 486, 494 (D.C. Cir. 1988), and that the harm in delaying disclosure is not necessarily redressed even if the information is provided at some later date, *see Byrd v. EPA*, 174 F.3d 239, 244 (D.C. Cir. 1999) ("Byrd's injury, however, resulted from EPA's failure to furnish him with the documents until long after they would have been of any use to him."). Here, however, the Court concludes that Plaintiff is not presently entitled to the information that it seeks, and accordingly, Plaintiff

cannot show that it has suffered an irreparable informational injury. To hold otherwise would mean that whenever a statute provides for potential disclosure, a party claiming entitlement to that information in the midst of a substantial public debate would be entitled to a finding of irreparable informational injury, which cannot be so. *See, e.g., Elec. Privacy Info. Ctr. v. Dep't of Justice*, 15 F. Supp. 3d 32, 45 (D.D.C. 2014) ("surely EPIC's own subjective view of what qualifies as 'timely' processing is not, and cannot be, the standard that governs this Court's evaluation of irreparable harm").

Finally, the equitable and public interest factors are in equipoise. As the Court recently held in a related matter, "[p]lainly, as an equitable and public interest matter, more disclosure, more promptly, is better than less disclosure, less promptly. But this must be balanced against the interest of advisory committees to engage in their work . . . ." *Lawyers' Comm. for Civil Rights Under Law v. Presidential Advisory Comm'n on Election Integrity*, No. CV 17-1354 (CKK), 2017 WL 3028832, at *10 (D.D.C. July 18, 2017). Here, the disclosure of a Privacy Impact Assessment may very well be in the equitable and public interest, but creating a right to such disclosure out of whole cloth, and thereby imposing an informational burden on the Commission where none has been mandated by Congress or any other source of law, is not.

IV. CONCLUSION

For all of the foregoing reasons, Plaintiff's [35] Motion for a Temporary Restraining Order and Preliminary Injunction is **DENIED WITHOUT PREJUDICE**.

An appropriate Order accompanies this Memorandum Opinion.

/s/
COLLEEN KOLLAR-KOTELLY
United States District Judge