DoD Instruction 8170.01

Online Information Management and Electronic Messaging

Originating Component:	Office of the Chief Information Officer of the Department of Defense
Effective:	December 31, 2018
Releasability:	Cleared for public release. Available on the Directives Division Website at http://www.esd.whs.mil/DD/.
Incorporates and Cancels:	DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012 Deputy Secretary of Defense Memorandum, "Ensuring Quality of Information Disseminated to the Public by the Department of Defense," February 10, 2003
Approved by:	Dana S. Deasy, Department of Defense Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance:

- Establishes policy, assigns responsibilities, and prescribes procedures for:
  - Conducting, establishing, operating, and maintaining electronic messaging services (including, but not limited to, e-mail) to collect, distribute, store, and otherwise process official DoD information, both unclassified and classified, as applicable.
  - Managing official DoD information on the DoD Information Network and other networks, i.e., online.
- Provides a compendium of policies and procedures critical to successful online information management and electronic messaging.

TABLE OF CONTENTS

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance:

a. Applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

(2) Official DoD information online, DoD electronic messaging, and DoD electronic messaging services, including when used or operated by non-DoD-entities.

(3) Contractors and other non-DoD entities that are supporting DoD mission-related activities, including accessing official DoD information online, conducting DoD electronic messaging, or operating electronic messaging, and electronic messaging services, to the extent provided in the contract or other instrument by which such authorized support or access is provided.

b. Does **not** apply to DoD Component use of electronic messaging specifically for penetration testing, communications security monitoring, defensive cyberspace operations, personnel misconduct and law enforcement investigations, and intelligence-related operations. Does not apply to information systems operated on behalf of the DoD but not used by DoD personnel. These activities remain subject to other legal and regulatory requirements such as records management.

1.2. POLICY. It is DoD policy that:

a. DoD electronic messaging and DoD electronic messaging services to access, collect, create, distribute, present, store, and process DoD information will be designed to be data-based and or information-centric whenever possible. Examples include:

(1) Updating business processes to allow access to and management of data as an asset.

(2) Distributing data via Web application programming interfaces (APIs).

(3) Decoupling data and presentation (i.e., information-centric instead of document-centric).

(4) Meta-data tagging.

(5) Device-agnostic access to information.

(6) Responsive design.

(7) Pervasive, global access to data and information through cloud services.

(8) Mobility.

b. DoD personnel must continue to innovate via electronic messaging services to achieve capabilities that are faster, better and less expensive, while simultaneously ensuring implementation of cybersecurity appropriate for the risks, and the magnitude of harm that could result from the loss, compromise, or corruption of the information.

c. DoD personnel must ensure that public DoD websites are operated in compliance with the laws and requirements cited in Office of Management and Budget (OMB) Memorandum M-17-06.

(1) Other DoD electronic messaging services must operate in compliance with OMB Memorandums M-06-16 and M-10-23.

(2) Detailed explanations and implementation guidance for compliance with these memorandums are provided at the Federal Web Managers Council Website at: https://digital.gov/.

d. DoD personnel must ensure that all unclassified DoD-controlled networks (e.g., Non-classified Internet Protocol Router Network, the Defense Research and Engineering Network) provide access to public, non-DoD-controlled electronic messaging services across all the DoD Components.

e. DoD personnel must digitally sign all electronic messaging when possible. All electronic messaging of controlled unclassified information should be encrypted when possible. Electronic messaging with classified information must be restricted to classified networks or encrypted with National Security Agency approved cryptography if not separately protected (e.g., by a protected distribution system).

f. DoD personnel must not use personal e-mail or other nonofficial accounts to exchange official information and must not auto-forward official messages to nonofficial accounts or corporate accounts. Exceptions are described in Paragraph 3.25.

g. DoD personnel must conduct online information management and electronic messaging, regardless of the information technology or format used, in compliance with applicable laws, regulations, this issuance and the references cited throughout this issuance.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO). In addition to the responsibilities in Paragraph 2.7., the DoD CIO:

a. Develops and coordinates DoD issuances for policy on the use, risk management, and compliance of official DoD information online, electronic messaging, and electronic messaging services.

b. Coordinates corrective action with the designated manager or responsible DoD or OSD Component head for DoD electronic messaging services not operated in compliance with this issuance.

c. Monitors emerging electronic messaging services developments to identify opportunities for use, including an assessment of costs and risks.

d. In coordination with the Assistant to the Secretary of Defense for Public Affairs (ATSD(PA)), oversees implementation of policy and procedures for ensuring quality of information the DoD distributes to the public.

e. In coordination with the ATSD(PA), serves as the OSD appeal authority to receive and resolve requests for appeal concerning the quality of information publicly distributed by OSD.

f. Provides records management guidance and oversight for the use of online information and electronic messaging, in accordance with DoDD 5144.02.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in Paragraph 2.7., the Director, DISA provisions and sustains the Defense Information System Network to host and serve Internet media via electronic messaging services.

2.3. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE. In addition to the responsibilities in Paragraph 2.7, the Under Secretary of Defense for Intelligence:

a. Ensures cybersecurity and operations security (OPSEC) vulnerabilities found on electronic messaging services are identified to and resolved by the designated manager or the responsible DoD or OSD Component head for resolution.

b. Coordinates corrective action for DoD electronic messaging services not operated in compliance with applicable cybersecurity and OPSEC policies with the responsible DoD and OSD Component heads and the DoD CIO, as necessary.

c. In coordination with the DoD CIO, integrates guidance regarding the responsible and effective use of electronic messaging services in OPSEC education, training, and awareness activities.

d. Provides policy, procedures, and oversight for DoD intelligence and intelligence-related activities that use electronic messaging services to collect information, in accordance with DoDDs 5148.13 and 5240.01, and DoD Manual 5240.01.

e. Provides guidance for the OPSEC reviews of DoD information intended for online distribution, sharing, storing, or other processing.

2.4. ATSD(PA). In addition to the responsibilities in Paragraph 2.7., the ATSD(PA):

a. Operates and maintains the federal agency public website for the DoD.

b. Hosts and operates registration systems for the addresses of public DoD electronic messaging services.

c. Provides guidance for official identifiers for external official presences (EOPs).

d. Develops and makes available education, guidance, and training for the responsible and effective use and management of EOPs.

e. In coordination with the DoD CIO, oversees implementation of policy and procedures for ensuring quality of information distributed to the public by the DoD, and serves as the primary information distribution activity (IDA) for OSD.

2.5. DIRECTOR, WASHINGTON HEADQUARTERS SERVICES. Under the authority, direction, and control of the Chief Management Officer of the Department of Defense and through the Director of Administration, Office of the Chief Management Officer, and in addition to the responsibilities in Paragraph 2.7., the Director, Washington Headquarters Services, includes the release of DoD information via electronic messaging services in the responsibilities and procedures published in DoDD 5230.09 and DoD Instruction (DoDI) 5230.29.

2.6. DIRECTOR, OVERSIGHT AND COMPLIANCE. Under the authority, direction and control of the Chief Management Officer of the Department of Defense, and as the DoD Senior Agency Official for Privacy (SAOP) conducts reviews identified in OMB Memorandum M-10-22 and maintains the agency Privacy Program Page as described in Paragraph 6.A. of OMB Memorandum M-17-06.

2.7. DOD AND OSD COMPONENT HEADS. The DoD and OSD Component heads:

a. Defend against malicious activity affecting DoD networks (e.g., distributed denial of service attacks, intrusions) and take immediate and commensurate actions, as required, to safeguard missions (e.g., temporarily limiting access to the Internet to preserve OPSEC, maintaining available bandwidth to meet operational demand).

b. Deny access to online services dedicated to prohibited content and prohibit authorized users from engaging in prohibited activity via electronic messaging services while at work or when using government equipment.

c. Establish a reporting process that will lead to corrective action for users who discover access to prohibited content on electronic messaging services used by the DoD or OSD Component.

d. Approve, as appropriate, establishment and registration of EOPs and official use of non-DoD-controlled and non-federal-controlled electronic messaging services.

e. Ensure all electronic messaging services used by the Component to publicly distribute unclassified DoD information are registered in compliance with the procedures in Paragraph 3.31.

f. Recognizing mission and resource priorities, assess the need to isolate, disconnect, terminate, or otherwise shut down electronic messaging services within Component jurisdiction that are not brought into compliance with applicable policies within 90 calendar days of identification or notification of noncompliance and for which no plan of action and milestones for correction is in place.

g. Establish basic quality standards that are appropriate to the nature and timeliness of information distributed to the public.

h. Develop and publish a review process that substantiates the quality of information publicly distributed by the Component.

i. Publish administrative mechanisms that allow affected persons to seek and obtain, where appropriate, timely correction of public DoD information maintained and distributed by the Component that may not be in compliance with the quality standards.

j. Designate the Component's public affairs activity or Military Department designee to receive complaint reports regarding information that may not comply with quality standards, maintain associated records of the claims received and their resolution, and forward copies of these records each fiscal-year to the ATSD(PA).

k. Ensure subordinate Component personnel are educated and trained in the responsible and effective use of electronic messaging services. Education and training must include, but not be limited to, accessibility, OPSEC, cybersecurity, records management, and information review for clearance and release authorization procedures.

l. Submit public Web application APIs to be included on the DoD Developers Website (https://www.defense.gov/developer/) and Data.gov's Web API catalog at https://data.gov.

m. Ensure all electronic messaging services used by the Component to distribute DoD information are assessed at least annually for compliance with this issuance.

n. Ensure that all nonpublic DoD information is collected, distributed, shared, stored, or otherwise processed on systems that are in compliance with DoDIs 8510.01 and 8582.01, and DoD 5220.22-M, and ensure DoD cybersecurity standards, controls, and enforcement are maintained.

o. Establish procedures for meeting the requirements of Paragraph 1.2.e.

2.8. DOD COMPONENT CIOS. The DoD Component CIOs:

a. Establish risk assessment procedures to evaluate and monitor Component use of current and emerging information technologies in order to identify opportunities for use and to assess risks.

b. Prepare and submit to the responsible Component head a plan of action and milestones for electronic messaging services within the Component jurisdiction that are not brought into compliance with applicable policies within 90 calendar days from identification of noncompliance. The plan should be developed in coordination with Component website administrators and aligned with mission and resource priorities,

c. In coordination with the Component public affairs office, assist in evaluating the intended use of non-DoD-controlled electronic messaging services for EOPs and other official purposes.

SECTION 3: PROCEDURES

3.1. GENERAL. DoD personnel must follow the requirements in this section when using electronic messaging services. These procedures do not:

a. Prevent unit commanders or DoD Component heads from providing stand-alone capabilities to allow access to non-DoD-controlled networks for mission or morale purposes.

b. Prohibit DoD personnel from using unofficial electronic messaging services from personal devices for personal purposes.

3.2. ACCESSIBILITY. Official electronic messaging services and online official DoD information must be accessible to disabled DoD personnel and disabled members of the public. Access must be comparable to that available to nondisabled individuals, in compliance with the requirements and alternatives in DoD Manual 8400.01. Current specific standards and methods are available at https://www.section508.gov/.

3.3. ADVERTISING AND ENDORSEMENT.

a. Non-U.S. Government (USG) advertising in electronic versions of nonappropriated fund products is governed by DoDIs 1015.08 and 1015.10 for military and civilian morale welfare and recreation, DoDI 1015.12 for DoD lodging, and DoDI 1330.21 for military exchange services. Non-USG advertising in electronic versions of Defense Commissary Agency products is governed by DoDI 1330.17.

b. Advertising in electronic versions of DoD newspapers, magazines, and civilian enterprise publications is governed by DoDI 5120.04.

c. For advertising outside the scope of Paragraphs 3.3.a. and 3.3.b. of this issuance, public electronic messaging services are considered publications. In accordance with DoD 5500.07-R, U.S. Congress Senate Publication 101-9, and DoDD 5500.07, association with non-USG sponsorships, advertisements, or endorsements must not adversely affect the credibility of DoD information. Specific advertising prohibitions include, but are not limited to:

(1) Do not insert or allow any advertisement by or for any private individual, firm, or corporation on public DoD electronic messaging services without specific statutory authority to do so. Do not imply DoD endorsement in any manner for any specific non-USG service, facility, event, or product.

(2) Do not accept remuneration of any kind (e.g., payment, reimbursement, reduced prices, gifts) in exchange for advertising, acknowledgement, or endorsement without specific authority to do so. Accepting remuneration may constitute an improper augmentation of appropriations in violation of Chapters 13 and 15 of Title 31, United States Code (U.S.C.).

(3) Do not insert or allow stand-alone non-USG graphics, logos, or aggrandizing statements such as "Powered by …," "Serviced by …," and "Designed by …" on public DoD-controlled electronic messaging services, or the DoD-controlled content area of other electronic messaging services prepared or produced with either appropriated or nonappropriated funds.

(a) Proprietary rights notices (including copyright and trademark notices) are not aggrandizing statements. Copyright notices are required, in accordance with Paragraph 3.8. of this issuance.

(b) Factual acknowledgement of partners, software, technology, and services used on a public DoD-controlled electronic messaging service may be included in descriptive information about the service or the organization, such as an "About Us" page. An acknowledgement should be carefully considered in the security risk assessment and risk mitigation measures for the service in accordance with DoDI 8510.01, and may not be used in any manner that supports the appearance of endorsement.

(c) Factual acknowledgement may include a corresponding non-USG graphic, logo, or trademark. This graphic, logo, or trademark may be used as a hyperlink to the corresponding non-USG website or service; however, the hyperlink must be disclaimed, in accordance with Paragraph 3.19.d.

d. Submit written requests to non-DoD-controlled electronic messaging service providers to block the display of any commercial advertisements, solicitations, or hyperlinks on EOPs and non-DoD-controlled electronic messaging service pages administered with official-use accounts if the provider would otherwise normally display such materials. Use the disclaimer in Figure 1 if required. If the non-DoD-controlled electronic messaging service provider is unwilling or unable to block the display of commercial advertisements, place the following message in a prominent location on each authorized page, as workable: "The appearance of commercial advertising and hyperlinks inserted by the host of this service does not constitute endorsement by the U.S. Department of Defense/[insert name of organization]."

3.4. ANNUAL ASSESSMENT. When ensuring compliance with this issuance, DoD and OSD Component heads must verify, at a minimum, that:

a. The existing access controls appropriately protect the information in accordance with Paragraphs 3.9 and 3.18.

b. The information distributed via public electronic messaging services has been reviewed, cleared, and authorized for public release, in accordance with DoDD 5230.09.

c. The DoD Component's information review for clearance and release authorization procedures are being followed, that the results correctly implement this issuance, and that copies of the documented review processes are maintained by the DoD Component's CIO.

d. Accessibility standards are incorporated to ensure compliance with DoD Manual 8400.01.

e. Online information and electronic messaging are managed, in accordance with DoDI 5015.02.

f. Corrective action is initiated and, as necessary, coordinated with the DoD CIO and United States Cyber Command, as delegated by United States Strategic Command, for any noncompliance discovered during the assessment.

3.5. BRANDING. Use official branding on electronic messaging services, in accordance with DoDD 5535.09 and other guidance issued by the ATSD(PA).

3.6. CLOUD. Use cloud services in accordance with the guidance at https://iase.disa.mil/cloud_security/Pages/index.aspx.

3.7. COLLECTING INFORMATION. Information collection via online surveys, forms, or other solicitations is subject to DoD 5240.1-R and 7750.07-M, DoDD 5148.13, DoDIs 1000.30, 1100.13, 7750.07, and 8910.01, DoD Manual 5240.01, and Chapter 91 of Title 15, U.S.C., as applicable to the intent or target audience of the collection. Specific applications of these regulations are governed by distinct policies and guidelines. The April 7, 2010 OMB Memorandums provide specific additional guidance to help determine when a collection is governed by or subject to the named sources.

3.8. COPYRIGHT. The application of Title 17, U.S.C., to specific situations is a matter for interpretation by legal counsel. It is essential to keep in mind that:

a. The DoD must recognize the rights of copyright owners pursuant to DoDD 5535.4.

b. Works of the USG prepared by DoD employees (or any officer or employee of the USG) as part of their official duties are not protected by copyright in the United States, in accordance with Title 17, U.S.C. This includes documents authored by DoD employees during official assignments to attend school as students.

c. Proper attribution must be made for all copyrighted material. Post a clear disclaimer detailing the copyrights retained by USG or non-USG contributors and identify the specific copyrighted work(s) (e.g., information, image, video, sound, design, code, template, service, technology) when placing copyrighted material on electronic messaging services.

3.9. CYBERSECURITY AND TRANSPORTATION LAYER SECURITY.

a. Comply with the appropriate requirements in DoDIs 8500.01, 8510.01, 8582.01; and DoD 5220.22-M, to ensure the electronic security of DoD information.

b. Display an approved, legally sufficient notice and consent banner, in accordance with DoDI 8500.01 and available at https://iase.disa.mil/, on private DoD electronic messaging services.

c. Configure DoD electronic messaging services to meet the public key enabling requirements listed in DoDI 8520.02. In accordance with the January 5, 2018 DoD CIO Memorandum, commercial device transportation layer security and code-signing certificates may be used on unclassified, external-facing, DoD websites and services used by non-DoD controlled devices, i.e., users of non-DoD desktops, laptops or other mobile devices. These certificates must meet the criterial for Extended Validation (equivalent to DoD medium assurance).

d. Implement a comprehensive, in-depth cybersecurity strategy for the security of Web services in accordance with the current versions of DISA's Security Technical Implementation Guides and Security Requirement Guides, available at https://iase.disa.mil/.

3.10. DATA.

a. Provide official DoD information, where feasible and appropriate, as datasets in machine readable, mobile-optimized format, and via Web APIs, in accordance with the May 23, 2012 Federal CIO Memorandum.

b. Architect new DoD electronic messaging services for openness and expose high-value data and content as Web APIs at a discrete and digestible level of granularity with metadata tags, in accordance with the May 23, 2012 Federal CIO Memorandum and the tagging concepts and standards found in DoDI 8320.07.

c. Create Web APIs, as appropriate, when current DoD electronic services are updated.

d. Guidance for developing Web APIs is available on the General Services Administration's (GSA) APIs in Government website at https://digital.gov/categories/api/.

e. Submit Web APIs to the DoD CIO for inclusion on the DoD Developers website at https://www.defense.gov/developer/ and Data.gov's Web API catalog.

3.11. DIGITAL ANALYTICS PROGRAM (DAP). Implement DAP code on all public DoD websites in accordance with OMB Memorandum M-17-06. Follow DAP implementation guidance at https://www.milsuite.mil/book/docs/DOC-46211.

3.12. DIGITAL SIGNATURE. DoD personnel must digitally sign electronic messages in accordance with the procedures in DoDI 8520.02.

3.13. DOD WEBSITE CONTACT INFORMATION. Link to contact information from all major entry points on DoD websites. Consolidate the following contact information for the organization managing the website on a single "Contact Us" page:

a. The organization's postal address.

b. The office telephone number(s), including numbers for any regional or local offices or toll-free numbers and telephone device for the deaf numbers, if available. If telephone device for

the deaf lines are not available, use an appropriate relay (e.g., the Federal Relay Service), as needed.

c. A means to communicate via e-mail (e.g., addresses, group mailbox).

d. Contact information to report availability, accessibility, technical and information quality problems.

e. A Privacy Act statement (PAS) or privacy advisory, as appropriate for the method of contact, in accordance with DoD 5400.11-R, DoDD 5400.11, and Paragraphs 3.26. and 3.27. of this issuance.

3.14. DOMAINS. Use Internet domain names established and approved in accordance with DoDI 8410.01 for all DoD-controlled electronic messaging services. The "*.mil*" Internet domain exists for the exclusive use of the DoD, and should be the primary address for DoD-controlled electronic messaging services.

3.15. ENCRYPTION. Encrypt electronic messages in accordance with the procedures in DoDI 8520.02 and Volume 4 of DoD Manual 5200.01.

3.16. FEDERAL INFORMATION SYSTEMS. DoD collection, distribution, storage, and other processing of information on federally-owned, operated, or controlled information systems (e.g., Intellipedia, Data.gov) are subject to the same policies and procedures as activities conducted on DoD-controlled systems.

3.17. IMAGE ALTERATION. Do not alter official DoD imagery beyond the allowances specified in DoDI 5040.02.

3.18. INFORMATION CONTROL, DISTRIBUTION, AND MARKING.

a. As applicable, comply with policies and procedures provided in DoD 5400.11-R, DoDDs 5122.05, 5210.50, 5230.09, 5230.25, 5400.11, and 5405.2, DoDIs 5030.59, 5200.01, 5230.24, 5230.27, 5230.29, and 8500.01, Volumes 1 through 4 of DoD Manual 5200.01, and OMB Memorandums M-06-16, and M-17-12.

b. Ensure and maximize the quality (i.e., objectivity, utility, integrity) of information distributed to the public, as appropriate to its nature and timeliness, consistent with Enclosure 2, Principles of Information, provided in DoDD 5122.05 and the guidance in Appendix 3A to this issuance.

3.19. HYPERLINKS.

a. Criteria. Establish hyperlinks only to information or services related to the performance of the DoD Component's function or mission and the purpose of the electronic messaging service.

(1) On public electronic messaging services, establish and publish objective criteria and guidelines for the selection and maintenance of hyperlinks to external information, along with the external hyperlinks disclaimer, as appropriate, following the guidance in Paragraph 3.19.d. of this issuance.

(2) Do **not** place hyperlinks or references to private USG electronic messaging services on public electronic messaging services. In certain circumstances, it may be appropriate to establish a hyperlink to a log-on page, provided that details about the contents of the private services are not revealed.

b. Frames and Other Direct Embedding. Assess and mitigate potential ethical, legal, and security risks (e.g., advertising, copyright, malware, trademark, other inappropriate or malicious behavior) when considering the use of frames and other technology to connect directly to and display content from other sites.

c. External Hyperlinks Disclaimer. Do **not** disclaim hyperlinks to USG electronic messaging services. Display or link to the quoted disclaimer in Figure 1 on public electronic messaging services that have non-USG hyperlinks, or through an intermediate "exit notice" page generated by the server whenever a request is made for any non-USG hyperlink.

Figure 1. External Hyperlinks Disclaimer

> "The appearance of hyperlinks does not constitute endorsement by the [insert sponsoring organization (i.e., Department of Defense, U.S. Army, U.S. Navy, U.S. Air Force, or U.S. Marine Corps)] of non-U.S. Government sites or the information, products, or services contained therein. Although the [insert sponsoring organization] may or may not use these sites as additional distribution channels for Department of Defense information, it does not exercise editorial control over all of the information that you may find at these locations. Such hyperlinks are provided consistent with the stated purpose of this website."

d. Mandatory Hyperlinks and Content. Verify all external hyperlinks to ensure continued provision of the hyperlink quality (i.e., correct address and objectivity, utility, and integrity of the content) intended by the DoD Component and expected by users. Relying solely on automatic hyperlink validation tools is not sufficient, and frequent manual review of the content at external hyperlinks is required.

(1) Authority, Mission, and Organization. Link to a description of the DoD or the DoD Component's organizational structure, mission, and statutory authority from major entry points (including homepages) on the DoD Federal Agency Public Website (https://www.defense.gov/) and the principal, public websites of the DoD Components, pursuant to OMB Memorandum M-17-06.

(2) Freedom of Information Act. The Internet home page of every DoD Component will link to the FOIA Requester Service Center for that DoD Component.

(3) Information Quality. Link to the DoD Information Quality website (https://dod.defense.gov/Resources/DoD-Information-Quality-Guidelines/).

(4) "No Fear Act" Data. Include a hyperlink specifically labeled "No Fear Act Data" on home pages of the DoD Federal Agency Public Website and the principal public websites of the DoD Components. This specific label must link to summary statistical data about equal employment opportunity complaints filed with DoD or with the DoD Components, as applicable, and written notification of whistleblower rights and protections pursuant to OMB Memorandum M-17-06 and Public Law 107-174 (also known as the "No Fear Act").

(5) Open Government. Link to the DoD Open Government website (https://open.defense.gov).

(6) Plain Writing. Link to the DoD Plain Writing website (http://www.esd.whs.mil/DD/plainlanguage/).

(7) Privacy Policy. Post or link to clear privacy policies on public DoD electronic messaging services, pursuant to OMB Memorandum M-17-06, at major entry points and those points or pages where personal information is collected from the public. Use the specific label "Privacy Policy." The privacy and security notice provided in Figure 2 may be tailored to improve readability and comprehension for the intended audience.

(8) Privacy Program. A link to the Department's Privacy Program page (defense.gov/privacy) must be included pursuant to OMB Memorandum M-17-06.(9) Strategic and Annual Performance Plans. Link to the DoD or the DoD Component's strategic and annual performance plans from major entry points to the DoD Federal Agency Public Website and the principal public websites of the DoD Components, consistent with OMB Memorandum M-17-06.

(10) USA.gov. Link to the USG's Official Web Portal, USA.gov, from major entry points to the DoD Federal Agency Public Website and, if deemed necessary, the principal public websites of the DoD Components, consistent with OMB Memorandum M-17-06.

Figure 2. Privacy and Security Notice

PRIVACY AND SECURITY NOTICE

1. [Name of service (e.g., "Website Title")] is provided as a public service by [name of the DoD Component(s)].

2. Information presented on this service, not identified as protected by copyright, is considered public information and may be distributed or copied. Use of appropriate byline, photo, and image credits is requested.

3. For site management, information is collected [Link "information is collected" to description of specific information. An example is provided after Paragraph 8. in this figure] for statistical purposes. This U.S. Government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, software programs are employed to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations and national security purposes, no other attempts are made to identify individual users or their usage habits beyond DoD websites. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration approved records schedule. [Agencies subject to DoD Directive 5240.01 must add the following sentence to this paragraph: "All data collection activities are in strict accordance with DoD Directive 5240.01."]

6. Web measurement and customization technologies (WMCT) may be used on this site to remember your online interactions, to conduct measurement and analysis of usage, or to customize your experience. The Department of Defense does not use the information associated with WMCT to track individual user activity on the Internet outside of Defense Department websites, nor does it share the data obtained through such technologies, without your explicit consent, with other departments or agencies, unless directed to do so in statute, regulation, or Executive order. The Department of Defense does not keep a database of information obtained from the use of WMCT. [If the DoD CIO has provided explicit written approval to use Tier III WMCT, cite that approval here.] General instructions for how you may opt out of some of the most commonly used WMCT is available at https://www.usa.gov/optout-instructions.

7. Unauthorized attempts to upload information or change information on this site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act (Section 1030 of Title 18, United States Code).

8. If you have any questions or comments about the information presented here, please forward them to [contact information to report both technical and information problems with the website specifically, including accessibility problems].

(11) Transparency Banner. As workable, display the standard transparency banner depicted in Figure 3 on EOPs and other official uses of non-DoD-controlled electronic messaging services.

Figure 3. Transparency Banner

"Welcome to the [name of DoD Component]'s [name of non-DoD-controlled electronic messaging service] page/presence. If you are looking for the official source of information about the [name of DoD Component], please visit [address of official website or other official information].

The [name of DoD Component] is pleased to participate in this open forum in order to increase government transparency, promote public participation, and encourage collaboration.
Please note that the [name of DoD Component] does not endorse the comments or opinions provided by visitors to this site. The protection, control, and legal aspects of any information that you provided to establish your account or information that you may choose to share here is governed by the terms of service or use between you and the [name of non-DoD-controlled electronic messaging service].

Visit the [name of DoD Component] contact page at [address of official website or other official information] for information on how to send official correspondence."

(12) Visual Information. Display a Public Use Notice of Limitations on all DoD Component website visual information galleries pursuant to DoDI 5410.20.

3.20. MOBILE CODE. Comply with DoDI 8500.01 for the distribution of software modules that are obtained from remote systems, transferred across a network, downloaded, and executed on a local system without explicit installation or execution by a recipient (e.g., JavaScript).

3.21. MOBILE OPTIMIZATION. Optimize DoD electronic messaging services to better ensure access to DoD information and services for mobile devices as part of lifecycle management, in accordance with the May 23, 2012 Federal CIO Memorandum. Include mobile optimization in new, updated versions of DoD electronic messaging services, as well as the requirement for optimized mobile functionality in the development process for new DoD electronic messaging services. Prioritize modernization based on customer feedback and analytics, and the frequency of use of the electronic messaging services.

3.22. MULTILINGUAL CONTENT. Provide website content in multiple languages in accordance with the guidance in Executive Order 13166.

3.23. OFFICIAL USE OF NON-DOD-CONTROLLED ELECTRONIC MESSAGING SERVICES. Do not use non-DoD-controlled electronic messaging services to process non-public DoD information, regardless of the service's perceived appearance of security (e.g., "private" Instagram accounts, "protected" tweets, "private" Facebook groups, "encrypted" WhatsApp messages). In addition to approving the establishment of EOPs, in accordance with Paragraph 2.7.d., and consistent with United States Office of Government Ethics Legal Advisory 15-03, the DoD and OSD Component heads may approve the establishment of non-DoD-controlled electronic messaging services accounts by authorized users for public communication related to assigned duties (e.g., recruiting) or any other purpose determined necessary and in the

interest of the USG. When engaging in official use of non-DoD-controlled electronic messaging services, DoD organizations should:

a. Limit use of non-DoD-controlled electronic messaging services to supplemental communication only. Do not establish or represent official-use accounts or pages as primary sources of DoD information.

(1) Organizations should provide individuals with comparable alternatives to non-DoD-controlled electronic messaging services through the organization's official website or other official means. For example, members of the public should be able to learn about the organization's activities and to communicate with the organization without having to join a third-party social media website.

(2) If an organization uses a non-DoD-controlled electronic messaging service to solicit feedback, i.e., ask for any information, the organization should provide an alternative government e-mail address where users can also send feedback.

b. Post, as practicable, a clear description of the purpose for using the service and that the DoD is the content provider.

c. Post, where applicable and practicable, hyperlinks to official DoD content on DoD-owned, -operated, or -controlled sites when official use of a non-DoD-controlled service references materials originating from an official DoD website.

d. Post hyperlinks to the organization's official public website.

e. Implement specific steps to protect individual privacy whenever the organization is using third-party websites and applications to engage with the public, in accordance with OMB Memorandum M-10-23.

f. Not conduct communication unrelated to assigned duties, functions, or activities via official-use accounts.

g. Liaise with public affairs and OPSEC staff to ensure organizational awareness of authorized, mission-related public communication.

h. Monitor the use of non-DoD-controlled electronic messaging services for security incidents (e.g., hacking), disclosure of personally identifiable information (PII), and fraudulent or objectionable use.

i. Review terms of service (ToS) agreements on non-DoD-controlled electronic messaging services to determine if they contain legally objectionable terms and conditions that must be amended or otherwise addressed prior to DoD use. The "standard" ToS used by the non-DoD-controlled electronic messaging service provider may contain legally objectionable terms and conditions that must be amended or otherwise addressed prior to DoD use. Additionally, non-DoD-controlled electronic messaging service providers may agree only to such amended terms and conditions for limited portions of their products and services.

(1) DoD personnel who establish an EOP or other official uses on a non-DoD-controlled electronic messaging service must verify whether the DoD CIO has signed an approved ToS for that service. Such ToS apply to DoD-wide use and operation of EOPs and other official uses. If the DoD CIO signs a ToS, there is no need for an additional ToS at the Component level. Signed and approved ToS are listed at https://dodcio.defense.gov/Social-Media/Terms-of-Service-Agreements/.

(2) If the DoD CIO has not signed a ToS agreement for a non-DoD-controlled electronic messaging service, establish a ToS agreement signed at the DoD Component level. The GSA provides ToS templates appropriate for federal government use (available at: https://digital.gov/) that must be adapted for DoD use if available for the desired service.

(3) ToS agreements implemented by the DoD do not cover personal, nonofficial accounts. The DoD will not be a party to, nor in any way be responsible for, individual obligations or agreements established with non-DoD-controlled electronic messaging services for personal, nonofficial use.

j. Consider using Go.USA.gov at https://go.usa.gov to create short .gov hyperlinks for official government addresses in the .gov and .mil domains when electronic messaging services (e.g., Twitter, Facebook) encourage shortened address hyperlinks to fit text and character limitations. For official government addresses in other domains, commercial address shorteners may be used, if available, however, because of the risk of harmful addresses masked in shortened URLs, many such services are blocked.

k. Use mission related contact information, such as official duty telephone numbers or postal and e-mail addresses, to establish official-use accounts, when such information is required by the electronic messaging service.

l. Establish official-use account pages for individuals and pages representing DoD organizations in the category "Government," and register organization names that begin with, "U.S. Department of Defense/[insert name of organization or name of component]" depending on the requirements of the specific non-DoD-controlled electronic messaging service. This requirement does not apply to creation of a specific account name, handle, or nickname.

m. Post, as practicable, the transparency banner described in Figure 3 when using a non-DoD-controlled electronic messaging service for official use, to ensure clear distinction between the collaborative forum or discussion board of the non-DoD-controlled electronic messaging service and the official information available on the DoD Component's website.

n. Include DoD records exchanged via non-DoD-controlled electronic messaging services in the DoD Component's records management program, consistent with Paragraph 3.30.

3.24. PLAIN WRITING. Web content must be written in accordance with the plain writing guidance in OMB Memorandum M-11-15 and online at https://www.plainlanguage.gov/.

3.25. PERSONAL USE OF NON-DOD-CONTROLLED ELECTRONIC MESSAGING SERVICES. DoD personnel may establish non-DoD-controlled electronic messaging accounts for personal, nonofficial use, in accordance with the following provisions:

a. DoD personnel may not use personal, nonofficial accounts, to conduct official DoD communications (policy in Paragraph 1.2.f.). Exceptions must meet the combined three conditions:

(1) Emergencies and other critical mission needs.

(2) When official communication capabilities are unavailable, impractical, or unreliable.

(3) It is in the interests of DoD or other USG missions.

b. Personal, nonofficial accounts may not be used to conduct official DoD communications for personal convenience or preferences. For example, the desire to only use a personal smartphone and not use one provided by DoD; or the preference for a commercially-provided webmail service, for example the Gmail client, over the Defense Enterprise E-Mail Outlook client are prohibited.

c. DoD personnel may use personal, nonofficial accounts to participate in activities such as professional networking, development, and collaboration related to, but not directly associated with, official mission activities as DoD personnel.

d. In accordance with United States Office of Government Ethics Legal Advisory 15-03, when conducting personal, nonofficial communication, DoD personnel must:

(1) Avoid the distribution and discussion of nonpublic information or the appearance of official sanction.

(2) Not disclose nonpublic information, or unclassified information that aggregates to reveal sensitive or classified information.

e. DoD personnel should use non-mission related contact information, such as personal telephone numbers or postal and e-mail addresses, to establish personal, nonofficial accounts, when such information is required.

f. Comply with records management procedures described Paragraph 3.30.

g. DoD personnel who are acting in a private capacity have the First Amendment right to further release or share publicly-released unclassified information through non-DoD forums or social media provided that no laws or regulations are violated. DoD personnel will not post comments or material that denigrates another military or civilian member of the DoD team. Some of the applicable laws and regulations are:

(1) Uniform Code of Military Justice.

(2) Joint Ethics Regulation, notably the provision that preparation activities are not conducted during normal duty hours or using DoD facilities, property, or personnel except as authorized (See DoD 5500.07-R).

(3) DoDD 1350.2.

(4) DoDD 1020.02E, notably the provision that equal opportunity is critical to mission accomplishment, unit cohesiveness and military readiness and that all are afforded equal opportunity in an environment free from harassment, including sexual harassment, and unlawful discrimination on the basis of race, color, national origin, religion, sex (including gender identity) or sexual orientation.

3.26. PAS.

a. Consistent with the requirements of DoD 5400.11-R, post a PAS when requesting an individual to furnish personal information to be included in a Privacy Act system of records. A PAS must be provided at the point of collection. For electronic collections acceptable methods of providing a PAS are a "click through" PAS or the provision of the PAS at the top of the collection page (similar to locating a PAS at the top of a paper form to be completed).

b. Comply with DoD 5400.11-R if collecting and maintaining personal information in a Privacy Act system of records.

c. If a PAS would be required for a paper-based solicitation, it is required for online solicitation, regardless of whether the site is a public or private electronic messaging service.

3.27. PRIVACY ADVISORY.

a. Provide a privacy advisory when requesting an individual to furnish personal information via a DoD website and the information is not maintained in a Privacy Act system of records. The privacy advisory informs the individual as to why the information is being solicited and how the information will be used.

b. Post the privacy advisory on the Web page where the information is being solicited or provided through a well-marked hyperlink. Providing the hyperlink via a statement, such as "Privacy Advisory: Please refer to the Privacy Policy that describes why this information is being collected and how it will be used," is satisfactory when linked directly to the applicable portion of the Privacy Policy, as required by Paragraph 3.19.d.(7).

3.28. PRIVACY IMPACT ASSESSMENT (PIA). Complete a PIA, in accordance with DoDI 5400.16, before activating electronic messaging services that interface with new or significantly altered information systems or electronic collections that collect, distribute, process, or consist of PII from or about members of the public, DoD personnel, or other USG personnel.

a. Post the results of the PIAs on the DoD Component's principal public website, in accordance with DoDI 5400.16.

b. In accordance with OMB Memorandum M-10-23, an adapted PIA is required whenever a DoD Component's use of a third-party website or application makes PII available to the DoD Component.

3.29. PRIVACY INCIDENTS. Report any loss of control, compromise, unauthorized disclosure, or unauthorized acquisition of PII, actual or suspected, in accordance with DoD 5400.11-R and Volume 4 of DoD Manual 5200.01.

3.30. RECORDS MANAGEMENT.

a. Manage all records, whether online or created and sent using official or personal electronic messaging services, in compliance with DoDI 5015.02.

b. Consistent with Section 2911 of Title 44, U.S.C., an officer or employee of an executive agency may not create or send a record using a nonofficial electronic messaging account unless such officer or employee:

(1) Copies an official electronic messaging account of the officer or employee in the original creation or transmission of the record; or

(2) Forwards a complete copy of the record to an official electronic messaging account of the officer or employee no later than 20 days after the original creation or transmission of the record.

3.31. REGISTRATION. Register the addresses and contact information for all public DoD electronic messaging services, including EOPs and other official uses of non-DoD-controlled electronic messaging services.

a. Register public websites at: https://www.defense.gov/Resources/Register-A-Site/.

b. Register public EOPs at: https://usdigitalregistry.digitalgov.gov/.

3.32. SEARCH.

a. Make information searchable and discoverable within appropriate boundaries based on sensitivity, classification and need to know.

b. Public websites must contain a search function that allows users to easily search content intended for public use. Explore integrating the no-fee services of GSA's DigitalGov Search (available at: https://search.gov/) to avoid creating and implementing duplicative search functions. In the case of very small sites, place a site map or subject index on the site to assist in locating DoD information.

3.33. WMCT. In accordance with OMB Memorandum M-10-22, DoD organizations may use WMCT (e.g., cookies) for the purpose of improving DoD electronic messaging services through conducting measurement and analysis of usage or through customization of the user's experience.

a. Restrictions. Unless directed to do so in statute, regulation, or Executive order, do not use such technologies:

(1) To track user individual-level activity on the Internet outside of the electronic messaging service from which the technology originates.

(2) To share the data obtained through such technologies with other federal agencies, the DoD Components, or other organizations, without a user's explicit consent.

(a) Explicit consent must include a notice of the purpose and ramifications of the technology being used, as well as an opt-in function to allow the users to signify they have read and understand the information and agree to the technology's use.

(b) Explicit consent could be achieved with a pop-up box and "agree" button that link to privacy policies and terms-of-use statements.

(3) To cross-reference any data gathered from WMCT against PII to determine individual-level online activity, without a user's explicit consent.

(4) To collect PII in any fashion without a user's explicit consent.

(5) For any like usages so designated by OMB.

b. Usage Tiers. The defined tiers for authorized use of WMCT are:

(1) Tier 1 – Single Session. This tier encompasses any use of single session WMCT.

(2) Tier 2 – Multi-session Without PII. This tier encompasses any use of multi-session WMCT when no PII is collected or processed (including when the Component is unable to identify an individual as a result of its use of such technologies).

(3) Tier 3 – Multi-session With PII. This tier encompasses any use of multi-session WMCT when PII is collected or processed (including when the component is able to identify an individual as a result of its use of such technologies).

c. Clear Notice and Personal Choice. Do not use WMCT that is difficult for the public to opt out of. Explain in Privacy Policy the decision to enable WMCT by default or not, and require users to make an opt-out or opt-in decision. Provide users who decide to opt out with access to information that is comparable to the information available to users who opt in.

(1) DoD Component-Side Opt-Out. Use of WMCT is encouraged and authorized, where appropriate, in order to establish that a user has opted out of all other uses of such technologies on the relevant domain or application. Such uses are considered Tier 2.

(2) Client-Side Opt-Out. If DoD Component-side opt-out mechanisms are not appropriate or available, instructions on how users can enable client-side opt-out mechanisms may be used. Client-side opt-out mechanisms allow the public to opt out of WMCT by changing the settings of a specific application or program on the public user's local computer. For example, public users may disable persistent cookies by changing the settings on commonly used Web browsers. A website's Privacy Policy should link to https://www.usa.gov/optout-instructions, which contains general instructions on how the public can opt out of some of the most commonly used WMCT.

(3) Tier 3 Restrictions. Use opt-in functionality when employing Tier 3.

d. Data Safeguarding and Privacy. Comply with DoD 5400.11-R and DoDD 5400.11 for all uses of WMCT.

e. DoD Components' Use of WMCT.

(1) Privacy Policy. DoD Components may use Tier 1 and Tier 2 WMCT, provided that the Components:

(a) Comply with OMB Memorandum M-10-22 and all other relevant policies.

(b) Provide to users clear and conspicuous notice of the use of WMCT in online Privacy Policy, as specified in Attachment 3 of OMB Memorandum M-10-22.

(c) Comply with DoD and DoD Component internal policies governing the use of such technologies.

(2) Privacy Office Review. The Director, Oversight and Compliance Directorate, Office of the Chief Management Officer of the Department of Defense, as the DoD SAOP must review all proposals by the DoD Components to engage in Tier 3 uses before implementation.

(3) Notice and Comment. Following DoD SAOP review for new proposals of Tier 3 uses or substantive changes to existing uses of such technologies:

(a) Solicit comment through the DoD Open Government Website at https://open.defense.gov/ for a minimum of 30 days. This notice and comment must include the DoD Component's proposal to use such technologies and a description of how they will be used.

1. Comments should, at a minimum, address the items in the Privacy Policy, as described in Attachment 3 of OMB Memorandum M-10-22.

2. DoD Components are exempt from this requirement if the notice-and-comment process is reasonably likely to result in serious public harm, with written approval from the DoD CIO.

(b) Review and consider substantive comments and make changes to their intended use of WMCT, where appropriate.

(c) The DoD Components must obtain explicit written approval from the DoD CIO and cite this approval in their online Privacy Policies. After obtaining the approval and completing notice and comment, as specified in Paragraph 3.33.e.(3), the DoD Components may use Tier 3 WMCT.

APPENDIX 3A: ENSURING THE QUALITY OF INFORMATION DISTRIBUTED TO THE PUBLIC

3A.1. UNDERLYING PRINCIPLES. Online communication increases the potential harm that can result from the public distribution of information that does not meet basic information quality standards. However, the variety of DoD information does not lend itself to a detailed, prescriptive, "one-size-fits-all" set of DoD-wide guidelines. DoD Components should not publicly distribute substantive information that does not meet a basic level of quality. An additional level of quality is warranted in those situations involving influential scientific, financial, or statistical information results. This additional level of quality requires that such information be "capable of being substantially reproduced."

3A.2. GUIDELINES.

a. In the spirit and intent of Public Law 104-13, also known and referred to in this issuance as the "Paperwork Reduction Act (PRA) of 1995," the guidelines apply to a wide variety of DoD IDA, including practices that have an impact on the acquisition, storage, and maintenance of the information to be publicly distributed. The guidelines are generic in order to apply to a variety of media, printed, electronic, or other forms of publication.

b. The guidelines are designed so that DoD Components can apply them in a common sense and workable manner. Components may incorporate the performance standards and procedures required by these guidelines into their existing information resources management and administrative practices rather than create new and potentially duplicative or contradictory processes. Components must ensure that their guidelines are consistent with these guidelines and their administrative mechanisms satisfy the standards and procedural requirements in these guidelines.

c. The quality of information publicly distributed by DoD Components must meet the attributes of utility, objectivity, and integrity, as defined in the Glossary.

d. In cases of public distribution of general scientific and research information, technical information that has undergone formal, independent, external peer review is presumptively objective. Components may rebut the presumed objectiveness, but must do so with persuasive information.

(1) The public distribution of scientific, financial, or statistical information that the DoD deems influential warrants a higher quality standard than that of peer review. To ensure the objectivity of influential scientific, financial, or statistical information, it must be capable of being substantially reproduced in accordance with commonly accepted scientific, financial, or statistical standards. This "reproducibility standard" ensures publicly distributed information is sufficiently transparent in terms of data and methods of analysis (i.e., that a replication feasibly could be conducted).

(2) Components responsible for public distribution of vital health and medical information must interpret the reproducibility and peer review standards in a manner appropriate to assuring the timely flow of vital information to medical providers, patients, health agencies and the public.

(3) With regard to information about risks to health, safety or the environment that DoD Components publicly distribute, DoD Components will adopt or adapt, as appropriate to the information in question, the quality principles of Section 300 Paragraphs g-1(A) and g-1(B) of Title 42, U.S.C. (also known as the "Safe Drinking Water Act of 1996").

e. These guidelines do not cover archival information publicly distributed by DoD Component libraries, which do not endorse the information they publicly distribute.

(1) Components have not authored this information or adopted it as representing DoD's or Components' views. By distributing this information, Components are simply ensuring that the public can have quicker and easier access to this information that is otherwise publicly available.

(2) These guidelines apply to information publicly distributed via a Component's Web page, but do not extend to the information publicly distributed by others that users obtain from following embedded hyperlinks on the Web page.

(3) These guidelines do not apply when a Component's presentation makes it clear that certain information is someone's opinion rather than fact or the Component's views, unless the Component represents the information as or uses the information in support of an official position of the Component. Components should use disclaimers to distinguish the status of such information.

f. Components' public distribution of information prepared by an outside party in a manner that reasonably suggests the Component agrees with the information is subject to the following guidelines:

(1) A Component does not initiate the public distribution of information when a Component-employed scientist or Component grantee or contractor publishes and communicates research findings in the same manner as academic colleagues, even if the Component retains ownership or other intellectual property rights because the Component paid for the research.

(2) To avoid confusion regarding whether a Component agrees with the information, the researcher should include an appropriate disclaimer in the publication or speech to the effect that the views expressed are his or her own and do not necessarily reflect the views of the Component.

g. If a Component directs a third party to publicly distribute information or retains the authority to approve the information before release, the Component has sponsored the public distribution of the information.

h. Specific types of information that are **not** subject to these guidelines include:

(1) Information with a distribution limited to government employees or Component contractors or grantees.

(2) Government information, including responses to requests pursuant to the Freedom of Information Act, Privacy Act, Federal Advisory Committee Act, or other similar laws, shared intra- or inter-Component or other department or agency.

(3) Correspondence with individuals or persons by the DoD Component.

(4) Information limited to subpoenas and adjudicative processes.

(5) Information that has previously been distributed to the public and is subsequently presented to Congress as part of the legislative or oversight processes, including testimony of officials, and information or drafting assistance provided to Congress in connection with pending or proposed legislation.

(6) Press releases and other information advising the public of an event or activity.

(7) Procedural, operational, policy, and internal manuals prepared for the management and operations of the Component that are not primarily intended for public distribution, including personnel notices such as vacancy announcements.

(8) Information that is not otherwise distributed to the public.

i. Any DoD agent may waive applicability of these DoD information quality guidelines for information publicly distributed in urgent situations, including imminent or credible threats to national defense and security.

3A.3. ADMINISTRATIVE MECHANISMS.

a. Unless otherwise established mechanisms exist, DoD Components must establish, and make public, administrative mechanisms to allow affected persons to seek and obtain, when proper documentation is provided, correction of information maintained and publicly distributed by the Component that does not comply with the DoD or OMB quality standards.

(1) Each Component must determine whether a person (e.g., group, organization, or corporation, as defined by the PRA of 1995), is or will be affected by the Component's information.

(2) These administrative mechanisms are not intended to replace or supersede existing mechanisms that may apply through other procedures. They also do not create substantive rights and are intended for administration only.

b. The correction process must be consistent with the genuine and valid needs of the Component and the DoD without disrupting Component and DoD processes. In making their determination of whether or not to correct information, Components may reject claims made in

bad faith or without justification and must undertake only the degree of correction that they conclude is appropriate for the nature and timeliness of the information involved.

c. Each Component's IDA will receive and resolve claims that are not addressed through another established process regarding information that does not comply with their quality standards. The IDA may consult with the Component's CIO during the process.

d. The IDA will allow affected persons to request correction to publicly distribute information, to the extent that such information is not accurate, clear, complete or unbiased.

(1) Persons must make claims in writing (electronic mail is encouraged), brief, simple, and containing, at a minimum:

(a) The publicly distributing organization.

(b) The location of the information.

(c) A description of the information to be corrected.

(d) The reason the information is not compliant with these guidelines.

(e) Copies of available documented evidence supporting the request.

(f) Information supporting the contention that the complainant is an affected person.

(2) A claim must not be resubmitted unless additional information is essential to process the request.

(3) Whenever practical, the Component will make a decision on whether to reject the claim or correct the information within 60 working days of receipt of the request. If the claim requires more than 60 working days to resolve, the Component will inform the requester that more time is required, and indicate the reason why and an estimated decision date.

e. The IDA will take one of the following actions on requests to correct information, consulting with the original public distributor of the information, as required:

(1) If the IDA agrees with any portion of a request, he or she will notify the public distributor of the information that the correction must be made, and will explain the substance of the requested correction in a manner associated with the extent of the complaint. The IDA must inform the requester, in writing, of the decision and the action taken.

(2) If the IDA disagrees with all or any portion of a request, he or she will inform the requester promptly in writing of the refusal to correct the information, the reason for refusal, and appeal procedures, as outlined in Paragraph 3A.3.g. of this issuance, including the name and address of the official to whom the requester should direct his or her appeal to.

(3) If the request for correction pertains to information originated, controlled, or maintained by another DoD Component or federal agency, the IDA will refer the request to the appropriate Component or agency and advise the requester of this in writing.

f. The following procedures will be used by the IDA when reviewing records under dispute:

(1) In response to a request for correction of information, the IDA will determine whether the requester has adequately supported the claim that the information is not accurate, clear, complete, or unbiased, and that the requester is an affected person.

(2) The IDA must limit the review of information to the aspect of the information that clearly bears on any determination to correct the information.

(3) If the IDA has received and responded to a previous claim concerning the information in question, he may reject as duplicative a new, similar request.

g. If the requester disagrees with the IDA's determination, he or she may file an appeal to the Component CIO, in writing, within 30 working days of notification of the determination.

(1) The Component CIO will process all appeals within 60 working days, unless the CIO determines that a fair review cannot be made within this time. If additional time is required at the expiration of the 60 day period, the CIO will notify the appellant of the delay in writing. The notification must include the reason for the delay and when the appellant may expect a decision on the appeal.

(2) If, after review, the Component CIO determines correction of the record as requested is unwarranted, the Component CIO will advise the appellant of the denial and explain the reason for the denial.

(3) If, after review, the Component CIO determines that the information should be corrected in accordance with the appellant's request, the Component CIO must direct the public distributor of the information to correct the information in question, and advise the appellant of the action taken.

3A.4. REPORTING REQUIREMENTS. On an annual fiscal-year basis, Components must submit copies of records to the ATSD(PA) about the claims received under the guidance in this appendix and their resolutions during the fiscal year. Components must submit these records no later than November 1. The ATSD(PA) will compile the records and submit the annual report to OMB. The format for the report to OMB is contained in Figure 4. Component records must include the number of claims received, how they were resolved (e.g., number corrected, denied, or pending appeal), and the number of staff-hours devoted to handling and resolving such claims and preparing documentation.

Figure 4. Template for DoD Information Quality Annual Report of Complaints Concerning Publicly-Distributed Information

Department of Defense Information Quality Annual Report of Complaints Concerning Publicly Distributed Information

Date: _____ For Fiscal Year Ending: _____

DoD Component (Service/Agency/Activity): _____

POC: Name/Phone/E-mail Address: _____

I. Number of complaints received: _____

A. Number of complaints substantiated as valid and corrected: _____

(1) Percentage of total received:_____

B. Number of complaints denied: _____

(1) Percentage of total received:_____

(2) Number of denied complaints appealed: _____

a. Number of appeals granted: _____

b Number of appeals denied: _____

c. Appeals pending as of end of FY: _____

C. For complaints involving "influential" scientific, financial or statistical information, provide a brief qualitative description of each complaint or category of complaints that are of a similar nature, and the resolution thereof.

II. Approximate staff-hours devoted to handling and resolving complaints and appeals and preparing reports: _____

GLOSSARY

G.1. ACRONYMS.

API	application programming interface
ATSD(PA)	Assistant to the Secretary of Defense for Public Affairs
CIO	Chief Information Officer
DAP	Digital Analytics Program
DISA	Defense Information Systems Agency
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
EOP	external official presence
IDA	information distribution activity
GSA	General Services Administration
OMB	Office of Management and Budget
OPSEC	operations security
PAS	Privacy Act statement
PIA	privacy impact assessment
PII	personally identifiable information
PRA	Paperwork Reduction Act
SAOP	Senior Agency Official for Privacy
ToS	terms of service
U.S.C.	United States Code
USG	U.S. Government
WMCT	Web measurement and customization technologies

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

access control. Technical measure or physical process used to grant or deny specific requests to obtain and use information and related information processing services. Also includes the use of a technical measure to enable customization or enhancement of a single user's experience.

advertisement or advertising. Material or information, regardless of media, publicly distributed in exchange for any remuneration or intended to promote any service, facility, or product of non-USG entities.

affected persons. Individuals who may benefit, be harmed, or otherwise be affected by publicly distributed information. This includes individuals seeking to address information about themselves, as well as individuals who use publicly distributed information.

agency. Any executive department, military department, government corporation, government-controlled corporation, or other establishment in the executive branch of the federal government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only OMB and the Office of Administration.

cybersecurity. Defined in DoDI 8500.01.

Defense Information System Network. Defined in DoD Dictionary of Military and Associated Terms.

decoupling data and presentation. Describing data clearly, and exposing it to other computers in a machine-readable format (commonly known as providing Web APIs). The data's description should ensure it has sound taxonomy (making it searchable) and adequate metadata (making it authoritative). Once the structure of the data is sound, various mechanisms can be built to present it to customers (e.g., websites, mobile applications, and internal tools) or raw data can be released directly to developers and entrepreneurs outside the organization.

distribute. To broadcast, publish, or to take other action to ensure availability beyond the control of the originating source or organization responsible for control of the information.

DoD-controlled. Defined in DoDI 8500.01.

DoD employee. Defined in DoD 5500.07-R.

DoD personnel. DoD employees, DoD contractor employees and non-DoD entities that are supporting DoD mission-related activities.

DoD website. Defined in DoD Dictionary of Military and Associated Terms.

electronic messaging. Online communication, including the exchange of Internet media, conducted via electronic messaging services.

electronic messaging services. Online communication capabilities, including websites, electronic mail, texting, chat, and related online communications methods.

EOP. Official public affairs activities, as defined in DoDI 5400.13, conducted on non-DoD-controlled electronic messaging services (e.g., Combatant Commands on Facebook).

exposure. Defined in DoDI 8320.02.

IDA. Any organization, office, entity, or activity, not limited to the public affairs activity that provides official information directly to the public.

influential. When used in the context of scientific, financial, or statistical information, the clear and substantial impact that public distribution of the information will have or does have on important public policies or private sector decisions. Each Component is authorized to define "influential" in ways appropriate, given the nature and multiplicity of issues for which the Component is responsible.

information-centric. Managing discrete pieces of open data and content which can be tagged, shared, secured and presented in the way that is most useful for the consumer of that information.

incident. Defined in OMB Memorandum M-17-12.

information. Defined in OMB Circular A-130.

information management. Defined in Joint Publication 3-0.

information technology. Defined in Joint Publication 3-0.

integrity. Refers to the security of information; namely, the protection of information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification.

Internet media. Files or messages delivered or acquired using any Internet protocol or supporting technology (e.g., Web pages, data or text, e-mail, video, audio, graphic, instant messages, chat).

metadata. Defined in DoDI 8320.02

mobile optimization. The process of ensuring electronic messaging services, data and information are usable on mobile devices such as smartphones and tablets.

nonofficial electronic messaging services. Online communication capabilities that are not intended to be used for official DoD information and are not owned, operated or controlled by the DoD. Examples include so-called "free services" such as Gmail and Hotmail, and "purchased services" such as Verizon and Comcast that an individual uses for his or her private, personal communications (i.e., for personal electronic messaging).

nonpublic information. Defined in DoD 5500.07-R.

objectivity. A measure of information quality related to accuracy, clarity, completeness, and unbiasedness and presented in the proper context. Sources of information are identified. Supporting data and models and errors and statistical ranges are included.

official use. Authorized communication or activities conducted as an assigned DoD personnel function. Official use includes emergency communications and communications that the DoD Component determines are necessary in the interest of the USG. Official use may include, when

approved by theater commanders in the interest of morale and welfare, communications by military members and other DoD personnel who are deployed for extended periods away from home on official DoD business.

official accounts. Capabilities specifically created and authorized for the primary purpose of exchanging official DoD information.

official DoD information. Defined in DoDD 5230.09.

online. Hosted on or conducted via the Internet, telecommunication networks, and computer systems.

PAS. Defined in DoD 5400.11-R.

personal electronic messaging. Individual communication or activity that is not conducted as an assigned DoD personnel function.

persons. Includes groups, organizations, and corporations as defined by the PRA of 1995.

PII. Defined in DoDD 5400.11.

private DoD electronic messaging service. An online DoD communication capability with access controls in place to limit availability of nonpublic information or exchanges of nonpublic information to specific audiences.

prohibited activity. Download, installation, or use of unauthorized software (e.g., applications, games, peer-to-peer software, movies, music videos, files); accessing pornography; posting comments and material that denigrates any military or civilian member of the DoD; unofficial advertising, selling, or soliciting; sending chain letters, offensive letters, mass e-mails, jokes, unnecessary pictures, and inspirational stories; improperly handling classified information; using DoD ISs to gain unauthorized access to other systems or networks; endorsing non-USG products or services; participating in any lobbying activity or engaging in any prohibited partisan activity; posting DoD information to external newsgroups, bulletin boards, or other public forums without authorization; and other uses incompatible with public service.

prohibited content. Applications, data, documents, files, software, or other information or materials acquired as a result of prohibited activity.

public DoD electronic messaging service. An online DoD communication capability used to collect, distribute, store, or otherwise process information that has been cleared and authorized for release to the public.

public DoD website. A DoD website used to collect, distribute, store, or otherwise process information that has been cleared and authorized for release to the public.

quality. An encompassing term comprising utility, objectivity, and integrity.

record. Defined in DoDI 5015.02.

responsive design. Defined in OMB Memorandum M-17-06.

review for clearance. Defined in DoDD 5230.09.

system of records. Defined in DoD 5400.11-R.

ToS. An agreement between a user and an electronic messaging service provider establishing the rights and responsibilities of the parties with respect to the use of the service. These agreements do not include procurement contracts and do not create financial obligations or liabilities on behalf of the USG.

utility. Refers to the relevance and timeliness of information to its intended users, including the public. In assessing the usefulness of information that a DoD Component distributes to the public, the Component needs to consider the uses of the information not only from the perspective of the Component but also from the perspective of the public.

website. A set of interconnected pages, services, and associated Internet media available at a URL and prepared and maintained as a collection of information and services by a person, group, or organization.

REFERENCES

DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended

DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1982, as amended

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD 5500.07-R, "Joint Ethics Regulation (JER)," August 1, 1993, as amended

DoD 7750.07-M, "DoD Forms Management Program Procedures Manual," May 07, 2008, as amended

DoD Chief Information Officer Memorandum, "Commercial Public Key Infrastructure Certificates on Public-Facing DoD Websites," January 5, 2018

DoD Directive 1020.02E, "Diversity Management and Equal Opportunity in the DoD," June 8, 2015, as amended

DoD Directive 1350.2, "Department of Defense Military Equal Opportunity (MEO) Program," August 18, 1995, as amended

DoD Directive 5122.05, "Assistant To The Secretary of Defense for Public Affairs (ATSD(PA))," August 7, 2017

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5148.13, "Intelligence Oversight," April 26, 2017

DoD Directive 5210.50, "Management of Serious Security Incidents Involving Classified Information," October 27, 2014, as amended

DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008, as amended

DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984, as amended

DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007, as amended

DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014

DoD Directive 5405.2, "Release of Official Information in Litigation and Testimony by DoD Personnel as Witnesses," July 23, 1985, as amended

DoD Directive 5500.07, "Standards of Conduct," November 29, 2007

DoD Directive 5535.09, "DoD Branding and Trademark Licensing Program," December 19, 2007

DoD Directive 5535.4, "Copyrighted Sound and Video Recordings," August 31, 1984, as amended

DoD Instruction 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD," August 1, 2012

DoD Instruction 1015.08, "DoD Civilian Employee Morale, Welfare and Recreation (MWR) Activities and Supporting Nonappropriated Fund Instrumentalities (NAFI)," December 23, 2005

DoD Instruction 1015.10, "Military Morale, Welfare, and Recreation (MWR) Programs," July 6, 2009, as amended

DoD Instruction 1015.12, "Lodging Program Resource Management," October 30, 1996

DoD Instruction 1100.13, "DoD Surveys" January 15, 2015, as amended

DoD Instruction 1330.17, "DoD Commissary Program," June 18, 2014, as amended

DoD Instruction 1330.21, "Armed Forces Exchange Regulations," July 14, 2005

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5030.59, "National Geospatial-Intelligence Agency (NGA) Limited Distribution Geospatial Intelligence (GEOINT)," March 10, 2015, as amended

DoD Instruction 5040.02, "Visual Information (VI)," October 27, 2011, as amended

DoD Instruction 5120.04 "DoD Newspapers, Magazines, Guides, and Installation Maps," March 17, 2015, as amended

DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended

DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, as amended

DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," November 18, 2016, as amended

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

DoD Instruction 5400.13, "Public Affairs (PA) Operations," October 15, 2008

DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended

DoD Instruction 5410.20, "Public Affairs Relations with For-Profit Businesses and Business Industry Organizations," September 29, 2016

DoD Instruction 7750.07, "DoD Forms Management Program," October 10, 2014

DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013

DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense," August 3, 2015, as amended

DoD Instruction 8410.01, "Internet Domain Name and Internet Protocol Address Space Use and Approval," December 4, 2015

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011

DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012, as amended

DoD Instruction 8910.01, "Information Collection and Reporting," May 19, 2014

DoD Manual 5200.01 Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

DoD Manual 5200.01 Volume 2, "DoD Information Security Program: Marking of Classified Information," February 24, 2012 as amended

DoD Manual 5200.01 Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

DoD Manual 5200.01 Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012, as amended

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

DoD Manual 8400.01, "Accessibility Of Information And Communications Technology (ICT)," November 14, 2017

Executive Order 13166, "Improving Access to Services for People with Limited English Proficiency," August 16, 2000

Federal Chief Information Officer, "Digital Government: Building a 21st Century Platform to Better Serve the American People," May 23, 2012 (also known as the "Digital Government Strategy")

Joint Committee on Printing U.S. Congress, Senate Publication 101-9, "Government Printing and Binding Regulations," February 1990

Joint Publication 3-0, "Joint Operations," January 17, 2017

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

Office of Management and Budget Circular A-130, "Managing Federal Information as a Strategic Resource," July 27, 2016

Office of Management and Budget Memorandum M-06-16, "Protection of Sensitive Agency Information," June 23, 2006[1]

Office of Management and Budget Memorandum M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies," June 25, 2010

Office of Management and Budget Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications," June 25, 2010

Office of Management and Budget Memorandum M-11-15, "Final Guidance on Implementing the Plain Writing Act of 2010," April 13, 2011

Office of Management and Budget Memorandum M-17-06, "Policies for Federal Agency Public Websites and Digital Services," November 8, 2016

[1] OMB memorandums are located at https://www.whitehouse.gov/omb/information-for-agencies/memoranda/

Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017

Office of Management and Budget Memorandum, "Information Collection under the Paperwork Reduction Act," April 7, 2010

Office of Management and Budget Memorandum, "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act," April 7, 2010

Public Law 104-13, "Paperwork Reduction Act of 1995," May 22, 1995

Public Law 107-174, "Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002," May 15, 2002 (also known as "The No Fear Act")

United States Code, Title 10, Chapter 47 (also known as the "Uniform Code of Military Justice (UCMJ)")

United States Code, Title 15

United States Code, Title 17

United States Code, Title 31

United States Code, Title 42

United States Code, Title 44

United States Office of Government Ethics Legal Advisory 15-03, "The Standards of Conduct as Applied to Personal Social Media Use"