PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Pentagon Facilities Parking Program

2. DOD COMPONENT NAME:

Washington Headquarters Service

3. PIA APPROVAL DATE:

04/06/22

WHS is the program manager for the Pentagon Facilities Parking Program, and the Pentagon Force Protection Agency ensures the system is operational as the system owners.

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

To manage the Pentagon Facilities Parking program for DOD civilians, military, and contractor personnel applying for and in receipt of Pentagon parking permit. Records are also used to ensure DOD military and civilian are not in receipt of both issued parking pass and mass transit benefit.
Type of information collected: Full name, SSN, work email address, rank /grade, work location/work phone, home zip code, organization affiliation, vehicle tag, and parking permit number.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Verification, identification, authentication (contractors are sponsored by a government agency within the Pentagon).

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Individuals can object to the collection of their PII; however, doing so would result in the denial of a parking permit.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Information is used to confer via license plate recognition (PFPA) that they are authorized to park at the Pentagon. It is also used to confirm they are not receiving double benefits such as parking privileges and Mass Transit Benefits.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

- [x] Privacy Act Statement
- [ ] Privacy Advisory
- [ ] Not Applicable

AUTHORITIES: 10 U.S.C. 2674, Operation and Control of Pentagon Reservation and Defense Facilities in National Capital Region; and Administrative Instruction 88, Pentagon Reservation Vehicle Parking Program, and E.O. 9397 (SSN), as amended.

PURPOSE(S): To manage the Pentagon Facilities Parking Program for DoD civilian, military, and contractor personnel applying for and in receipt of Pentagon parking permits. Records are also used to ensure DoD military personnel and civilians are not in receipt of both an issued parking pass and mass transit benefits.

ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as listed in the applicable system of records notice located at: https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570582/dwhs-d04/

DISCLOSURE: Voluntary; however, failure to provide the requested information may result in denial of Parking privileges at the Pentagon

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X]	Within the DoD Component	Specify.	WHS parking management office / mass transit program
[X]	Other DoD Components	Specify.	PFPA for parking enforcement, and DoD Component parking representatives (read only access)
[ ]	Other Federal Agencies	Specify.	
[ ]	State and Local Agencies	Specify.	
[ ]	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
[ ]	Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

[X]	Individuals	[ ]	Databases
[ ]	Existing DoD Information Systems	[ ]	Commercial Systems
[ ]	Other Federal Information Systems		

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

[X]	E-mail	[X]	Official Form (*Enter Form Number(s) in the box below)*
[X]	Face-to-Face Contact	[ ]	Paper
[ ]	Fax	[ ]	Telephone Interview
[ ]	Information Sharing - System to System	[ ]	Website/E-Form
[ ]	Other *(If Other, enter the information in the box below)*		

DD1199. If the form is emailed, it is encrypted. Face to Face contact to update license plates.

k. 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 must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier DWHS D04

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. **What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?**

(1) NARA Job Number or General Records Schedule Authority. GRS 5.6, item 130 (DAA)

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Cut off and destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner

m. **What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 U.S.C. 2674, Operation and Control of Pentagon Reservation and Defense Facilities in National Capital Region; and Administrative Instruction 88, Pentagon Reservation Vehicle Parking Program, and E.O. 9397 (SSN), as amended.

n. **Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☐ No ☒ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

WHS/DD/Information Management Office is in the process of updating the OMB control number that expires, 31 March 2022.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

☐ Biometrics	☐ Birth Date	☐ Child Information
☐ Citizenship	☐ Disability Information	☐ DoD ID Number
☐ Driver's License	☐ Education Information	☐ Emergency Contact
☐ Employment Information	☐ Financial Information	☐ Gender/Gender Identification
☐ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☐ Mailing/Home Address	☐ Marital Status	☐ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☒ Official Duty Address	☒ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☐ Personal E-mail Address	☐ Photo
☐ Place of Birth	☐ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☒ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☐ If Other, enter the information in the box below	

Home zip code, organization affiliation, license plate number, state of registration of the vehicle, and permit number.

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☒ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

Yes, SSN Justification Memo and was submitted 1 Feb 2022 to PCLTD.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

11. Legacy System Interface.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

WHS is actively working to replace the legacy parking database with a new parking system that will use the DoD ID number in lieu of the SSN.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☒ Yes ☐ No

New WHS parking system in development in 2022-2023. Implement the new WHS parking system in 2024.

b. What is the PII confidentiality impact level[2]? ☐ Low ☒ Moderate ☐ High

[1] The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2] Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [ ] Cipher Locks
- [x] Combination Locks
- [ ] Key Cards
- [ ] Security Guards
- [ ] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [ ] If Other, enter the information in the box below

Employees must have swipe access to enter the parking office. The next entrance requires number code. Files are kept in cabinets with key lock.

(2) Administrative Controls. *(Check all that apply)*

- [ ] Backups Secured Off-site
- [ ] Encryption of Backups
- [ ] Methods to Ensure Only Authorized Personnel Access to PII
- [ ] Periodic Security Audits
- [ ] Regular Monitoring of Users' Security Practices
- [x] If Other, enter the information in the box below

Emailed DD1199 and scanned ones are saved to DD1199 folder with limited access.

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [ ] Encryption of Data at Rest
- [x] Firewall
- [ ] Role-Based Access Controls
- [ ] Virtual Private Network (VPN)
- [x] Command Access Card (CAC)
- [ ] Encryption of Data in Transit
- [ ] Intrusion Detection System (IDS)
- [ ] Used Only for Privileged (Elevated Roles)
- [ ] If Other, enter the information in the box below
- [ ] DoD Public Key Infrastructure Certificates
- [ ] External Certificate Authority Certificates
- [ ] Least Privilege Access
- [x] User Identification and Password

To access the parking system an individual must be authorized to have a parking account.

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

[X]	Yes, DITPR	DITPR System Identification Number	DITPR 17285
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[ ]	Yes, RMF tool	RMF tool Identification Number	
[ ]	No		

If "No," explain.

NOTE: WHS is the primary user of the parking database and controls the information collected and stored in this system; however, PFPA maintains the system with updates and patches to ensure it continues operating.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

[X]	Authorization to Operate (ATO)	Date Granted:	11/22/2021
[ ]	ATO with Conditions	Date Granted:	
[ ]	Denial of Authorization to Operate (DATO)	Date Granted:	
[ ]	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT Investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

[ ] Yes [ ] No

If "Yes," Enter UII _____ If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3]Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Regina M. Grant	(1) Title	Director, Pentagon Services Division
(2) Organization	Washington Headquarters Services	(3) Work Telephone	703-614-6443
(4) DSN		(5) E-mail address	regina.m.grant6.civ@mail.mil
(6) Date of Review	04/01/22	(7) Signature	GRANT.REGINA.MAXINE.1049840205 Digitally signed by GRANT.REGINA.MAXINE.1049840205 Date: 2022.04.01 16:02:22 -04'00'
b. Other Official ***(to be used at Component discretion)***		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
c. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
d. Component Privacy Officer (CPO)	Jeanette S. Whiten	(1) Title	Privacy Officer
(2) Organization	Washington Headquarters Services	(3) Work Telephone	571-372-0937
(4) DSN		(5) E-mail address	jeanette.s.whiten.civ@mail.mil
(6) Date of Review	04/04/22	(7) Signature	WHITEN.JEANETTE.S.1042898518 Digitally signed by WHITEN.JEANETTE.S.1042898518 Date: 2022.04.04 07:22:16 -04'00'

e. Component Records Officer	Ronald R. McCully Jr	(1) Title	OSD Records Manager
(2) Organization	Washington Headquarters Services	(3) Work Telephone	571-372-0473
(4) DSN		(5) E-mail address	ronald.r.mccully2.civ@mail.mil
(6) Date of Review	04/05/22	(7) Signature	MCCULLY.RONALD.R.JR.1173976310 Digitally signed by MCCULLY.RONALD.R.JR.1173976310 Date: 2022.04.05 15:12:16 -04'00'
f. Component Senior Information Security Officer or Designee Name	Vince Tur-Rojas	(1) Title	Director, Security Management
(2) Organization	Pentagon Force Protection Agency	(3) Work Telephone	(703) 692-0459
(4) DSN		(5) E-mail address	vicente.r.tur-rojas2.civ@mail.mil
(6) Date of Review:		(7) Signature	TUR-ROJAS.VICENTE.R.II.1121687794 Digitally signed by TUR-ROJAS.VICENTE.R.II.1121687794 Date: 2022.04.14 15:34:51 -04'00'
g. Senior Component Official for Privacy (SCOP) or Designee Name	Luz D. Ortiz	(1) Title	Chief, Records and Declassification Division
(2) Organization	Washington Headquarters Services	(3) Work Telephone	(571)372-0478
(4) DSN		(5) E-mail address	luz.d.ortiz.civ@mail.mil
(6) Date of Review	4/06/2022	(7) Signature	ORTIZ.LUZ.D.1182242906 Digitally signed by ORTIZ.LUZ.D.1182242906 Date: 2022.04.06 08:39:47 -04'00'
h. Component CIO Reviewing Official Name	Dr. James Day	(1) Title	Executive Director, Security Integration and Technology
(2) Organization	Pentagon Force Protection Agency	(3) Work Telephone	703-692-4940
(4) DSN		(5) E-mail address	james.a.day76.civ@mail.mil
(6) Date of Review	04/06/22	(7) Signature	DAY.JAMES.ARLIE.1297625639 Digitally signed by DAY.JAMES.ARLIE.1297625639 Date: 2022.04.18 16:49:33 -04'00'

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.