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:

Privilege Management Program-2

2. DOD COMPONENT NAME:

Pentagon Force Protection Agency

3. PIA APPROVAL DATE:

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
- ☒ 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
- ☒ 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 collect and maintain records related to Pentagon Facility access and perimeter control, including visitor security and management. To issue individual facility/installation access credentials, and to verify individual's identity. The records will be continuously vetted against DoD Identity Management Capability Enterprise Service Application (IMESA), which may be accessed by other physical access control systems for further verification at other sites to be determined. The system may also be used for law enforcement purposes for verification and validation of person's recent and current police records.

Types of personal information about individuals collected in the system are as follows:
Name, Identification Number (ID), Social Security Number (SSN), Department of Defense ID (DoD ID) number, Federal Personal Identity Verification (PIV) Card Holder Unique Identifier (CHUID), I-9 lists of verification documents, date and place of birth, employment category (i.e. government, foreign, contractor), citizenship, gender, photograph, digital certificates, biometric images and templates (e.g., fingerprint and iris), home and work address, personal and work e-mail addresses and telephone numbers, name of DoD sponsoring office, background investigation type and completion date, date of issue and expiration of facility and installation access credentials, access level, previous facility pass issuances, and authenticating official, and information that reflects time of entry and exit from a facility.

Privately owned vehicle year, make/model, color, vehicle identification number (VIN), state and license plate 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. To manage physical access to the Privilege Management Program-2 (PMP-2), in accordance with Homeland Security Presidential Directive 12, its supporting documentation and implementation guidance issued by the Office of Management and Budget (OMB) and the Department of Defense (DoD).

e. Do individuals have the opportunity to object to the collection of their PII? ☒ 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.

DISCLOSURE: Voluntary, however, refusal to furnish requested information may result in the inability to access PFPA controlled facilities using Common Access Card (CAC), Personal Identity Verification (PIV), or Pentagon Facility Alternative Credential (PFAC) cards.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☐ Yes ☒ No

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

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

The Pentagon Force Protection Agency requires collection of information from individuals to grant them access to PMP. Once they have provided the information, they do not have the opportunity to consent to the specific uses of their PII.

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.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

DD 2249 PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 2674, Operation and Control of Pentagon Reservation and Defense facilities in National Capital Region; DoD Directive (DoDD) 1000.25, DoD Personnel Identity Protection (PIP Program; DoDD 8521.01E, Department of Defense Biometrics; DoD Instruction 5200.08,Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoD 5200.08-R, Physical Security Program; DoD 5105.68, Pentagon Force Protection Agency; OSD Administrative Instruction 30, Force Protection on the Pentagon Reservation; 32 CFR 234, Conduct on the Pentagon Reservation, as amended; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): To facilitate verification of background investigations for individuals applying for access to DoD buildings in connection with their official duties.

ROUTINE USE(S): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended. The DoD Routine Use(s) can be found in the applicable system of records notice, DPFPA 01, Pentagon Facilities Access Control System; located at: https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570581/dpfpa-01/

DISCLOSURE: Voluntary, however, refusal to furnish requested information may result in the inability to access PFPA controlled facilities using Control Access Card(CAC), Personal Identification Verification or Pentagon Facility Access Card (PFAC) cards.

PMP VMS PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 2674, Operation and Control of Pentagon Reservation and Defense facilities in National Capital Region; DoD Directive (DoDD) 1000.25, DoD Personnel Identity Protection (PIP) Program; DoDD 8521.01E, Department of Defense Biometrics;DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB);DoD 5200.08-R, Physical Security Program; DoD 5105.68, Pentagon Force Protection Agency; OSD Administrative Instruction 30, Force Protection on the Pentagon Reservation; 32 CFR 234, Conduct on the Pentagon Reservation, as amended; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): To maintain a listing of personnel who are authorized to access Pentagon facilities and verify identity of approved individuals to access such facilities and offices.

ROUTINE USE(S): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended. The DoD Routine Use(s) can be found in the applicable system of records notice, DPFPA 01, Pentagon Facilities Access Control System; located at: https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570581/dpfpa-01/

DISCLOSURE: Voluntary. However, failure to provide requested information or participate in this process may result in PFPA being unable to verify your identity and connect it with your facility access privileges resulting in your being unable to access the facility or spaces within it.

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

☒ Within the DoD Component	Specify.	Pentagon Force Protection Agency (PFPA)
☒ Other DoD Components	Specify.	Defense Manpower Data Center (DMDC), Defense Forensic & Biometric Agency
☒ Other Federal Agencies	Specify.	Government Printing Office (GPO)
☐ State and Local Agencies	Specify.	N/A
☒ 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.	MC Dean, Bowhead, and all contractors must sign nondisclosure form before being granted access to the system. Privacy FAR clauses are included in the contract. PWS contract states contractor shall comply with: NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations" which covers Privacy regulations.

☐ 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)*

☒ 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)*

☐ E-mail
☒ Official Form (*Enter Form Number(s) in the box below)*
☒ 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)*

Individuals needing access will provide PIV card information and fill out access card request form. Information will be processed through kiosk machines and/or through a Pentagon sponsored RAPIDS Issuance Facility.
DD 2249 and PMP VMS.

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier DPFPA 01 Pentagon Facilities Access C

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. DAA-GRS-2017-0006-0016

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

(3) Retention Instructions.

Temporary: Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use. (DAA-GRS-2017-0006-0016)

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; 32 CFR 234, Conduct on the Pentagon Reservation, as amended; DoD Directive (DoDD) 5105.68, Pentagon Force Protection Agency (PFPA); DoDD 8521.01E, DoD Biometrics; DoD Instruction (DODI) 1000.25, DoD Personnel Identity Protection (PIP) Program; DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoDI 5525.19, DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Databases (TSDB); DoD 5200.08-R, Physical Security Program; OSD Administrative Instruction 30, Force Protection on the Pentagon Reservation; Directive-Type Memorandum (DTM) 09-12, Interim Policy Guidance for DoD Physical Access Control; 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.

The OMB license for this system is 0704-0328 originally cleared 8/29/1991. It is currently in the process of being updated.