

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:

Personnel Account Maintenance (PAM)

2. DOD COMPONENT NAME:

Under Secretary of Defense for Personnel and Readiness

3. PIA APPROVAL DATE:

06/15/2026

Deputy Assistant Secretary of Defense (DASD) for Military Community and Family Policy (MC&FP)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

- ☐ From members of the general public ☐ From Federal employees
- ☒ from both members of the general public and Federal employees ☐ 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.

The Personnel Account Maintenance (PAM) system supports MC&FP's maintenance of records associated to users of MC&FP information systems and databases. The system allows MC&FP to track and manage user identification, credentialing, authentication, and authorization, facilitating reliable, secure, and auditable managed access across the broad portfolio of MC&FP digital resources. The system, thereby, enables a secure, trusted environment where users can access authorized resources, including services, information systems, and data.

The information collected and maintained in the system includes: full name, DoD ID, organization/component, position/title, phone number, and email address.

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)

Collection of personally identifiable information (PII) is required for user identification and verification for the purpose of account creation and management.

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.

Yes, individuals are provided a Privacy Act Statement at the point of collection and have the opportunity to object to the collection of their PII. Failure to provide the requested PII, however, will prevent account creation and system access.

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.

No, however, once collected the information will only be used for the specific purpose stated above and outlined in the Privacy Act Statement provided at the point of collection and below in g.

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

AUTHORITY: 10 U.S.C. 2224, Defense Information Assurance Program and DoD Instruction 8520.03, Identity Authentication for Information Systems.

PURPOSE: To allow for account creation, facilitate managed access, and enable user authentication.

ROUTINE USES: Disclosure of records are generally permitted under 5 U.S.C. 522a(b) of the Privacy Act of 1974, as amended. Pursuant to 5 U.S.C. 522a(b)(3), records may be disclosed as a routine use to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records. A complete list of routine uses may be found in the applicable System of Records Notice, DoD 0015, Enterprise Identity, Credential, and Access Management (ICAM) Records at: <https://www.federalregister.gov/documents/2022/12/16/2022-27356/privacy-act-of-1974-system-of-records>

DISCLOSURE: Voluntary. However, failure to provide requested information will prevent account creation and system access.

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

☐ Within the DoD Component

Specify.

☐ Other DoD Components (i.e. Army, Navy, Air Force)

Specify.

☐ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

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.

Fusion Technology Strategies and Aretum in performance of contractual duties and responsibilities. The contract requires baseline risk management and cybersecurity controls be implemented to ensure PII is safeguarded, and includes clauses 52.224-1 and 52.224-2.

☐ 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)

☐ In-Person Contact

☐ Paper

☐ Fax

☐ Telephone Interview

☐ Information Sharing - System to System

☒ Website/E-Form

☐ Other (If Other, enter the information in the box below)

DD2875, System Authorization Access Request (SAAR)

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

DoD 0015

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

I. 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 3.2 Item 30, DAA-GRS-2013-0006-0003

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

(3) Retention Instructions.

Temporary; Destroy when business use ceases.

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 statute 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. 2224, Defense Information Assurance Program and DoD Instruction 8520.03, Identity Authentication for Information Systems

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.

0704-0630, "System Authorization Access Request Form," 07/31/2028