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:

DoD Enterprise Identity, Credential, and Access Management (DoD E-ICAM)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

05/21/24

Cyber Security Analytics Directorate

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
- [x] 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
- [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.

Department of Defense Enterprise Identity Credential and Access Management (DoD E-ICAM) is the primary enterprise identity service solution for DISA on an unclassified network. DoD E-ICAM system creates a single user record, consolidating all pertinent data associated with the individual under one (1) account. DoD E-ICAM capture and maintain a record of names, digital signatures, accesses granted, and other identifiers from authoritative sources to provide and maintain a record of access management to DoD systems and resources. This record of access management shall include Financial Management and Reporting Records and Information Systems Security Records. This information is used to audit application access and validate those individuals that have the appropriate level of access required when attempting to access DoD applications and systems.

DoD E-ICAM consists of three systems: DoD E-ICAM Identity Provider (IdP), DoD E-ICAM Master User Record (MUR), DoD E-ICAM Automated Account Provisioning (AAP)

DoD E-ICAM systems are hosted in the Microsoft Cloud Azure tenant DEAS INF, referred to as the 'GFUD Tenant'. What the general populous commonly refers to as GFUD or GD is a subsystem of the DoD E-ICAM IdP built across multiple subscriptions and virtual machines in the 'GFUD Tenant' alongside of the virtual machines and subscriptions hosting SailPoint, Radiant Logic, DIU, systems.

DOD E-ICAM IdP collects users data includes individual's name (last name, first name, middle Initial); unique identifiers including DoD identification number (DoD ID Number), other unique identifier (not SSN), FASC-N, login name, legacy login name, and persona user-name; object class; rank; title; job title; persona type code (PTC); primary and other work e-mail addresses; persona display name (PON); work contact information, including administrative organization, duty organization, department, company (derived), building, address, mailing address, country, organization, phone, fax, mobile, pager, DSN phone, other fax, other mobile, other pager, city, zip code, post office box, street address, Country Of Citizenship (CTZP _CTRY _CD), state, room number, assigned unit name, code and location, attached unit name, code and location, major geographical location, major command, assigned major command, and base, post, camp, or station; US government agency code; service code; personnel category code; non-US government agency object common name; user account control; information technology service entitlements; and PKI certificate Information, including FASN-C, PIV Auth certificate Issuer, PIV Auth certificate serial number, PIV Auth certificate principal name, PIV Auth certificate SubjectAlternativeName, PIV Auth Thumbprint, PIV Auth Issuer, PlV Auth Common name, ID certificate issuer, ID certificate serial number, ID certificate principal name, ID Thumbprint, ID CN, signature certificate e-mail address, Signature Subject Alternative Name UPN, Signature Thumbprint, Signature Issuer, Signature serial number, Signature CN, Encryption (Public Binary Certificate), Encryption Thumbprint, CertificateIssuer, Encryption Serial Number, Encryption CN, distinguished name, PKI login identity, e-mail encryption certificate, and other certificate information.

DoD E-ICAM AAP provides an automated System Authorization Access Request (SAAR) service that leverages authoritative data sources to pre-populate data.

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)*

DoD E-ICAM MUR collects user identity data from IdP such as full name, home address, country citizenship, unit address, duty work phone number, CAC issue date, CAC expiration date, user encryption certificate, persona username, branch of service, EDIPI number, etc. to populate the DoD E-ICAM Master User Record (MUR).

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.

PII data is required to implement and operate DoD information technology (IT). If the data was not available for a specific individual, then that individual would not be able to access key new components of DOD IT such as business systems access, which are require for individuals to complete their work. DoD E-ICAM cannot remove an individual's data, since it does not collect PII directly from the individual, but rather obtains data elements from other established systems that are approved to collect these PII data.

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.

DoD E-ICAM provides a Privacy Act statement to its users which notifies the individual about the authority to collect the information requested, the purposes for which it will be used, other routine uses of the information, and the consequences of declining to provide the information. The consent banner is presented on the Mission Partner SailPoint website upon gaining access.

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. Chapter 8-Defense Agencies and Department of Defense Field Activities; DoD Directive (DoDD) 5105.19, Defense Information Systems Agency (DISA); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Enterprise User Data Management Plan for Persons and Personas; and DoD Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS); DoDI 5200.46-DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC) and DoDI 8520.03-Identity Authentication for Information Systems.

Principle Purpose: Department of Defense Enterprise Identity, Credential, and Access Management (DoD E-ICAM) System is a DoD Enterprise Identity Service that creates a single user record, consolidating all pertinent data associated with the individual under one (1) account. Its principle purpose is to capture and to maintain a record of names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

Routine Uses: The information in this system may be disclosed as generally permitted under 5 U.S.C Section 552a(b) of the Privacy Act of 1974, as amended. It may also be disclosed outside of the Department of Defense (DoD) to the Federal Reserve Banks to verify authority of the appointed individuals to issue Treasury checks. In addition, other Federal, State and local government agencies, which have identified a need to know, may obtain this information for the purpose(s) identified in the DoD Blanket Routine Uses published at: https://dpcld.defense.gov/Privacy/About-the-Office/DoD-Federal-Privacy-Rule/Appendix-C/.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of system access request or may preclude appointments.

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.	DISA
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	All DoD Military Departments and Defense Agencies
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	epartment of Veterans Affairs and the U.S. Department of State Other federal Agencies that can access the information from the DoD Enterprise White Pages: DHS - Department of Homeland Security, CIA - Central Intelligence Agency/ Director of National Intelligence, DOJ - Department of

Justice, DOC - Department of Commerce, DOE - Department of Energy, NASA - National Aeronautics and Space Administration, U.S. Department of the Treasury, NRC - Nuclear Regulatory Commission, GAO - Government Accountability Office, and the U.S. Department of State.

☒ State and Local Agencies

Specify. All users appropriately sponsored for access to supported applications

☒ 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. GDIT: OTA contract includes privacy clauses (Privacy Act of 1974, Public Law 93-579, December 31,1974 (5 U.S.C.552a)

☐ 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

Identity Synchronization Services (IdSS), Defense Information Security System (DISS), Defense Civilian Personnel Data System (DCPDS), Army Master Identity Directory (AMID), Air Force Directory Services (AFDS), DISA Corporate Management Information System (CMIS), DISA, Global Directory, Enterprise Identity Attribute Service (EIAS), Global Federated User Directory (GFUD), Defense Manpower Data Center Backend Attribute Exchange (DMDC BAE), Enterprise Mission Assurance Support Service (eMASS), Navy Federation, Defense Manpower Data Center (DMDC)

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)*

Terms of Service agreements are established between DoD Enterprise Identity, Credential, and Access Management (DoD E-ICAM), Department of Defense military organizations, federal, state, and local agencies.

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://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-GRS2013-0003-0001(Financial management records only), DAA-GRS-2013-0006-0001, DAA-GRS-2013-0006-0003, DAA-GRS-2013-0006-0004

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

(3) Retention Instructions.

Longer retention is authorized if required for business use for this disposition authority. Disposition is 10 years after the final invoice or Intra-Government Payment and Collection or other similar documentation. Note: This is an increase over the NARA six-year minimum retention standards for these record types. To support the beginning balances in the Department's Fiscal Year 2018 financial audit, documentation from greater than six years prior will be required. Thus, documentation must be retained for 10 years, the life of our longest lived (non-no-year) funding.

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.

The following authority allow DoD E-ICAM to collect data:
- 5 U.S.C. 30 1, Departmental Regulation;
- 10 U.S.C. Chapter 8-Defense Agencies and Department of Defense Field Activities;
- DoD Directive (DoDD) 5105.19 Defense Information Systems Agency (DISA);
- DoD Directive 1000.25;
- DoD Personnel Identity Protection (PIP) Program;
- DoD Enterprise User Data Management Plan for Persons and Personas, August 11, 2010;
- DoD Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS), March 11, 2009;
- DoDI 5200.46-DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC) ;
- DoDI 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.

OMB Control Number: 0704-0415;
Expiration Date: None