# 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:**

DEPARTMENT OF DEFENSE NETWORK-UNCLASSIFIED CLOUD (DoDNet-U Cloud)

**2. DOD COMPONENT NAME:**

Defense Information Systems Agency

**3. PIA APPROVAL DATE:**

02/13/24

## 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.**

DoDNet-U Cloud is a DoD wide cloud-based 4ENO Infrastructure as a Service (IaaS), Platform as a Service (PaaS,) and Software as a Service (SaaS) architecture supporting DoDNet that hosts development, testing and production systems.

**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)*

The Dept. of Defense Network Domain System supports the assigned DoD customer base for its Enterprise Level Information Management requirements by granting the individual system user access through the usage of the DoD ID credential and the utilization of the assigned Common Access Card (CAC). The information is managed by the passing of the associated credential embedded in the CAC card which is then verified against the user profile in Active Directory. The established processes and procedures are part of the authentication process for all categories of DoD personnel and contractor employees accessing the DoDNet.
The DoDNet-U Cloud does not collect or utilize PII for any other reason than authentication. However, data that transverses the system may contain PII and It's up to the individual program to secure the information of its own system.

**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.

A user may object to the collection or 'use' of their PII by choosing not to access the DoDNet. However, access to this network is required as part of conducting DoD business. Individual users' PII may transverse the entirety of the network based upon an individual's use of programs on the network. Collection of PII in those cases is covered by the individual program's PIA.

**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.

A user may object to the collection or 'use' of their PII by choosing not to access the DoDNet. However, access to this network is required as part of conducting DoD business. Individual users' PII may transverse the entirety of the network based upon an individual's use of programs on the network. Collection of PII in those cases is covered by the individual program's PIA.

**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: 5 U.S.C. Section 301; 10 U.S.C. Sections 1074(c)(1) and 1095(k)(2); 10 U.S.C. chapter 147; 50 U.S.C.

chapter 23; E.O. 9397; E.O. 10450, as amended.
PRINCIPAL PURPOSE(S): To apply for the Common Access Card and/or DEERS Enrollment; control access to and movement in or on DoD installations, buildings, or facilities; regulate access to DoD computer systems and networks; and verify eligibility, if authorized, for DoD benefits or privileges. To authenticate the identity of the authorizing/ verifying official for security or auditing purposes.
ROUTINE USE(S): To Federal and State agencies and private entities, as necessary, on matters relating to utilization review, professional quality assurance, program integrity, civil and criminal litigation, and access to Federal government and contractor facilities, computer systems, networks, and controlled areas.
DISCLOSURE: Voluntary; however, failure to provide information may result in denial of a Common Access Card; non-enrollment in the Defense Enrollment Eligibility Reporting System (DEERS); refusal to grant access to DoD installations, buildings, facilities, computer systems and networks; and denial of DoD benefits and privileges if otherwise authorized.
[For contractor personnel who are not required to have a National Agency Check only: Failure to provide a social security number will not result in denial of the Card, enrollment in DEERS, access to facilities or networks, or if eligible for, receipt of DoD benefits and privileges (other than non-emergency health care services), provided alternative means of identification (original birth certificate, passport, etc.) are voluntarily furnished upon request. However, submission of alternative identification may cause substantial delays; and if not provided, may result in denial of the Card, nonenrollment, refusal of access, and denial of benefits and privileges.]

**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. | Army, Navy, Air Force, Marine Corp, Coast Guard, Fourth Estate Organizations |
| ☒ | Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)* | Specify. | Dept of Veterans Affairs |
| ☐ | 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. | Leidos:<br>FAR 39.105 Privacy - ensures that contracts for information technology address protection of privacy in accordance with the Privacy Act and Part 24.<br>52.217-8 - option to extend services (not to exceed 6 months) via a -8 |
| ☐ | 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 | | |

DOD ID numbers are stored in AD (Active Directory).

**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)* | | |

**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 K890.14

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 3.1 and 3.2 various

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

(3) Retention Instructions.

GENERAL RECORDS SCHEDULE 3.1: General Technology Management Records
• 001 Technology management administrative records.
Disposition Instruction:
Temporary. Destroy when 5 years old, but longer retention is authorized if needed for business use.
• 020 Information technology operations and maintenance records.
Disposition Instruction:
Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.
• 030 Configuration and change management records.
Disposition Instruction:
Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.
GENERAL RECORDS SCHEDULE 3.2: Information Systems Security Records
• 010 Systems and data security records.
Disposition Instruction:
Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.
• 020 Computer security incident handling, reporting and follow-up records.
Disposition Instruction:
Temporary. Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.
• 030 System access records.
Disposition Instruction:
Temporary. Destroy when business use ceases.
• 040 System backups and tape library records.
Disposition Instruction:
Temporary. Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later.
• 060 PKI administrative records.
Disposition Instruction:
Temporary. Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.
• 062 PKI transaction-specific records.
Disposition Instruction:
Temporary. Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the appropriate CA and after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule, or in the case of permanent records, when the record is transferred to NARA legal custody. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period.

**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.

5 U.S.C. App. 3, Inspector General Act of 1978; 5 U.S.C. Chapter 90, Long-Term Care Insurance; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 53, Miscellaneous Rights and Benefits; 10 U.S.C. Chapter 54, Commissary and Exchange Benefits; 10 U.S.C. Chapter 58, Benefits and Services for Members being Separated or Recently Separated; 10 U.S.C. Chapter 75, Deceased Personnel; 10 U.S.C. 2358, Research and Development Projects; 10 U.S.C. Chapter 49 Section 987, Terms of Consumer Credit Extended to Members and Dependents: Limitations; 20 U.S.C. 1070a (f)(4), Higher Education Opportunity Act; 31 U.S.C. 3512(c), Executive Agency Accounting and Other Financial Management Reports and Plans; 42 U.S.C. 18001 note, Patient Protection and Affordable Care Act (Pub. L. 111-148); 52 U.S.C. 20301, Federal Responsibilities; 50 U.S.C. Chapter 23, Internal Security; 50 U.S.C. 501, Servicemembers Civil Relief Act; 38 CFR part 9.20, Traumatic injury protection; 38 U.S.C. Chapter 19, Subchapter III, Service members' Group Life Insurance; DoD Directive 1000.04, Federal Voting Assistance Program (FVAP); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 1015.09, Professional U.S. Scouting Organization Operations at U.S. Military Installations Overseas; DoD Instruction 1100.13, DoD Surveys; DoD Instruction 1241.03, TRICARE Retired Reserve (TRR) Program; DoD Instruction 1241.04, TRICARE Reserve Select (TRS) Program; DoD Instruction 1336.05, Automated Extract of Active Duty Military Personnel Records; DoD Instruction 1341.2, Defense Enrollment Eligibility Reporting System (DEERS) Procedures; DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural or Manmade Disasters; Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors; DoD Instruction 7730.54, Reserve Components Common Personnel Data System (RCCPDS).

**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