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:

Identity Synchronization Service (ldSS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

Enterprise Directory Services (EDS)

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.

Purpose: The ldSS will populate and maintain persona-based user objects in DoD enterprise-level Domain Controllers, such as the Active Directory Enterprise Application and Services Forest (AD EASF) being implemented by DISA to provide DoD Enterprise E-Mail, workspace and collaboration tools, file storage, and office applications. In addition, DISA may use the ldSS to populate and maintain persona data elements in DOD Component networks and systems, such as directory services and account provisioning 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)*

Mission-related use

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.

These PII data are required to implement and operate DoD Information Technology (IT). If data were not available for a specific individual, then that individual would not be able to access key new components of DoD IT, such as Enterprise E-Mail, which are required for individuals to do their work. The ldSS 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. An example is DEERS, which is provided by the Defense Manpower Data Center (DMDC), who functions as the DOD Data Wholesaler for these data. These systems provide individuals the capability to review and update their data, such as at the DMDC Personnel Portal where users can review their data, enter or provide certain data, and be directed to other organizations and systems to update other data (such as in local DOD Component Human Resources (HR) systems).

Individuals seeking to determine whether information about themselves is contained in this system of records can e-mail disa.meade.esd.list.idam-eds@mail.mil or address written inquiries to Defense Information Systems Agency (DISA), Enterprise Services Directorate, PO Box 549, Fort George G Meade, MD 20755-0549.

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 ldSS 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. An example is DEERS, which is provided by the Defense Manpower Data Center (DMDC), who functions as the DOD Data Wholesaler for data.

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

ldSS 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. An example is DEERS, which is provided by the Defense Manpower Data Center (DMDC), who functions as the DoD Data. Wholesaler for this data, DMDC typically provided directly by the user or by DoD Component systems. Other DoD Component, such as Human Resources IT systems. Individuals are provided a Privacy Act Statement and Privacy Advisories at that point prior to collection or update of their their data in accordance with standard procedures for those systems. In addition, Privacy Advisories are provided when users access DoD end-user devices which, in turn, are used to access the application(s) use of ldSS to establish user accounts (Exchange, SharePoint, vOffice, etc.).

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.	Enterprise Application and Services Forest (EASF)
☒ Other DoD Components	Specify.	DoD Component providers of directory services and account provisioning and access control.
☒ Other Federal Agencies	Specify.	Other federal Agencies that can access the information from the DoD Enterprise White Pages: DHS, CIA, DNI, DOJ, DOC, DOE, NASA, Dept of Treasury, NRC, GAO, Dept of State.
☐ State and Local Agencies	Specify.	NA
☐ 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.	NA
☐ Other (e.g., commercial providers, colleges).	Specify.	NA

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

NA

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)*

NA

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 DoD

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.

NA

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 5.2, item 020

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

(3) Retention Instructions.

Disposition Authority DAA-GRS2017-00030002. System's sole function is to receive and integrate data from two or more other systems and export the resultant product to yet another independent system. Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

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 allows Identity Synchronization Service (ldSS) to collect the following data:
- 5 U.S.C. 301, Departmental Regulation;
- 10 U.S.C. chapter 8; DOD Directive 5105.19, Defense Information Systems Agency (DISA);
- Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS), March 11, 2009.

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