PRIVACY IMPACT ASSESSMENT (PIA)

For the

Identity Synchronization Service (IdSS)/Active Directory Enterprise Application and Services Forest (AD EASF)
Defense Information Systems Agency (DISA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	14473
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier K890.14

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number 0704-0415

Enter Expiration Date

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

The following authority allows Identity Synchronization Service (IdSS)/Active Directory Enterprise Application and Services Forest (AD EASF) 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);
- DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program;
- DoD Enterprise User Data Management Plan for Persons and Personas, August 11, 2010;
- Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS), March 11, 2009.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Purpose: The IdSS 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) implemented by DISA to provide DoD Enterprise E-Mail, workspace and collaboration tools, file storage, and office applications. In addition, DISA may use the IdSS to populate and maintain persona data elements in DoD Component networks and systems, such as directory services and account provisioning systems.

Categories: For DoD persona, these include 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 username; object class; rank; title; job title; persona type code (PTC); primary and other work e-mail addresses; persona display name (PDN); 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 Subject Alternative Name, PIV Auth Thumbprint, PIV Auth Issuer, PIV 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, Certificate Issuer, Encryption Serial Number, Encryption CN, distinguished name, PKI login identity, e-mail encryption certificate, and other certificate information.

For VA personnel, these include individual's name (last name, first name, middle initial); other unique identifier (not SSN); primary and other work e-mail addresses; administrative organization code; duty sub-organization code; Persona E-Mail Address; e-mail encryption certificate.

Purpose: The AD EASF will control access and provide contact information for users of DoD Enterprise E-Mail, workspace and collaboration tools, file storage, and office applications.

Categories: Include 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 username; object class; rank; title; job title; persona type code (PTC); primary and other work e-mail addresses; persona display name (PDN); 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 Subject Alternative Name, PIV Auth Thumbprint, PIV Auth Issuer, PIV 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, Certificate Issuer, Encryption Serial Number, Encryption CN, distinguished name, PKI login identity, e-mail encryption certificate, and other certificate information.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Access to the type and amount of data is governed by privilege management software and policies developed and enforced by Federal government personnel. Defense-in-Depth methodology is used to protect the repository and interfaces, including (but not limited to) multi-layered firewalls, Secure Sockets Layer/Transport Layer Security (SSL/TLS) connections, access control lists, file system permissions, intrusion detection and prevention systems and log monitoring. Complete access to all records is restricted to and controlled by certified system management personnel, who are responsible for maintaining the IdSS system integrity and the data confidentiality.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. DoD Enterprise Application and Services Forest (EASF)/ Identity Synchronization System (IdSS) and applications using the AD EASF for control access and to provide contact information for users of DoD Enterprise E-Mail, workspace and collaboration tools, file storage, and office applications.

☒ **Other DoD Components.**

Specify. DoD Component providers of directory services and account provisioning systems.
Individual users who will access user contact information maintained in the AD EASF, such as by using the address list features of Microsoft Outlook.

☒ **Other Federal Agencies.**

Specify. 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.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

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

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

These PII data are required to implement and operate DoD information technology (IT). If these 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 IdSS/AD EASF 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-provided 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.eis.list.idam-eds@mail.mil or address written inquiries to Defense Information Systems Agency (DISA), Services Directorate (SE), P.O. Box 549, Ft. Meade, MD 20755-0549.

j. 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.

These PII data are required to implement and operate DoD information technology (IT). If these 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. In addition, this system 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. The AD EASF 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-provided 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.eis.list.idam-eds@mail.mil or address written inquiries to Defense Information Systems Agency (DISA), Services Directorate (SE), P.O. Box 549, Ft. Meade, MD 20755-0549.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒	**Privacy Act Statement**	☒	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.

IdSS 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. DMDC data are typically provided directly by the user, or by DoD Component systems that collect data, such as DoD Component Human Resources IT systems. Individuals are provided a Privacy Act Statement and Privacy Advisories at the point where they enter and update their data in accordance with standard procedures for these systems. In addition, Privacy Advisories are provided when users access DoD end-user devices which, in turn, are used to access the applications that use the IdSS to establish user accounts (Exchange, SharePoint, vOffice, etc.).

AD EASF 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 (primarily through the Identity Synchronization Service (IdSS)). An example is DEERS, which is provided by the Defense Manpower Data Center (DMDC), who functions as the DoD Data Wholesaler for these data. DMDC data are typically provided directly by the user, or by DoD Component systems that collect data, such as DoD Component Human Resources IT systems. Individuals are provided a Privacy Act Statement and Privacy Advisories at the point where they enter and update their data in accordance with standard procedures for these systems. In addition, Privacy Advisories are provided when users access DoD end-user devices which, in turn, are used to access the applications that use the AD EASF for access control and to obtain user contact information (Exchange, SharePoint, vOffice, etc.).

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.