PRIVACY IMPACT ASSESSMENT (PIA)

For the

ECHO
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: 9989
- ☐ **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: K890.15 DoD

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

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 ECHO to collect PII data:

- 5 U.SC 301, Departmental Regulation
- DoD Directive 5105.19, Defense Information Systems Agency (DISA)
- DoD Chief Information Officer Memorandum for Director, Defense Information Systems Agency (DISA)
- Enterprise Directory services Roadmap for the Department of Defense, 2 May 2005

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.

The system will be used to correlate user activities across a variety of cybersecurity-related records for the purpose of attack detection and insider threat analysis. In particular, the information system makes it possible to relate records containing various user identifiers (i.e. email addresses, DoD ID, name, etc...) to one another for the purpose of tracking a user's activities across multiple, disjoint systems.

Data collected for each user includes:
First and last name, branch of service, agency, duty location, email address, duty station phone number, rank, and Common Access Card (CAC) information.

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

The data contains personally identifiable information that would allow someone to learn work-related contact information for the user, as well as basic attributes related to their DoD position (i.e. rank, service, etc...).

The data is moved from the unclassified Active Directory Enterprise Application and Services Forest (AD EASF) environment to a CND Analytics Resource environment with significant auditing and security procedures consistent with FOUO Sensitive data use, including the use of strong access controls, multi-layered firewalls, and secure network protocols. Intermediary servers used to facilitate transfer to the CND Analytics Resource environment will not allow any user interaction except for system management and administration staff, and will perform automated bulk transfers of user data to the CND Analytics Resource environment when that data is updated in the AD EASF environment.

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. USCC, AFCERT, NCDOC, MARCET, 1st IO CMD, DLA CERT, SecDef, DCC, JFHQ-DODIN

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. NSA TOC

☐ **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.

Individuals may object to the collection of PII by not providing the requested information, however this information is required to gain access to the DoD Enterprise email environment.

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

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.

Individuals are provided a consent from during enrollment in the DoD Enterprise email program, and they may choose not to sign it, however, this consent is required to gain access to the DoD Enterprise email environment.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

PRIVACY ACT STATEMENT

Authority for maintenance of system: 5 U.S.C. 301, Departmental Regulation; DoD Directive 5105.19, Defense Information Systems Agency (DISA).

Purpose(s): Form is used to establish a Local Area Network (LAN) Account. This includes the level of security clearance and level of access to sensitive or classified information that has been authorized. Information is used by commanders, supervisors, and security managers to ensure that individuals who are granted access to sensitive or classified information have been properly investigated, cleared and have a definite need-to-know.

Routine Use(s): The DoD Blanket Routine Uses published at the beginning of the DISA's compilation of System of Records Notices applies to this system. In addition to those disclosures generally permitted under 5 USC 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside of DoD as a routine use pursuant 5 USC 552a(b)(3) as follows: 'Blanket Routine Uses' set forth at the beginning of the DISA's compilation of systems of records notices applies to this system.

Disclosure: Voluntary; however, failure to provide the information may impede access to the DoD Enterprise email environment and ECHO Network Enclave.

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.