PRIVACY IMPACT ASSESSMENT (PIA)

For the

Joint Enterprise Directory Services (JEDS)
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: 10686
- ☒ **Yes, SIPRNET** Enter SIPRNET Identification Number: 10686
- ☐ **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 K890.10

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 authority allows DISA Joint Enterprise Directory Services (JEDS) to collect the following data

- 5 U.S.C. 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.

Purpose(s): To provide a DoD Directory Services capability offering a single source from which to obtain identity and contact information about Combatant Command, Service, and Agency personnel as well as an enterprise level attribute service. JEDS will support the warfighter's mission by providing access, via controlled interfaces, to DoD personnel contact information and when requested by approved DoD applications, to identity attributes, and to support authorization decisions.

Categories of records in the system: Individual's name, Electronic Data Interchange Person Identifier (EDI PI), other unique identifier (not SSN), rank, title, personnel type, DoD component, DoD sub-component, Non-DoD agency, position title, business email address, and display name(s), office commercial and Defense System Network (DSN) phone and fax numbers, business mobile phone numbers, Internet Protocol (IP) phones, business location and mailing addresses, DoD PKI email encryption certificate, distinguished name from source record(s), directory publishing restrictions, country of citizenship, U.S. citizenship status, DoD job skill, language skill and occupational codes, reserve component code, segment termination code, assigned unit name, code and location, attached unit name, code and location, major geographical location, major command, assigned major command, job series, billet code, and pay grade.

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

Safeguards: 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 connections, Directory 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 JEDS 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. For DoD white pages and email Global address list (GAL)

☒ **Other DoD Components.**

Specify. For DoD white pages and email Global address list (GAL)

☐ **Other Federal Agencies.**

Specify.

☐ **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.

Notification procedure: Individuals seeking to determine whether information about themselves is contained in this system of records should email jeds2@disa.mil or address written inquiries to Defense Information Systems Agency, Directory Services Branch, PEO-IAN/IA42, P.O. Box 4502, Arlington, VA 22204-4502. Requests must include the individual's full name, rank, grade or title, component affiliation, work email address, telephone number, assigned office or unit, and complete mailing address. Email requests must be digitally signed with the requester's valid DoD or ECA identity certificate.

Request for how to correct or where JEDS collected the individual's information can be submitted either to the JEDS PMO as indicated above or as troubletickets to the GDS/JEDS DECC OKC Helpdesk at (800) 490-1643 or okc-dodost@csd.disa.mil
JEDS cannot remove an individual's entry; since it does not generate the information, rather it is generated within their respective DoD Components HR and IT systems and automatically collected by the JEDS automated harvesting process. An individual would have to contact their respective DoD Component's HR and/or IT offices or departments using their respective Component's Privacy guidelines to object to JEDS collecting their work related contact and identity information. Their DOD Components can then either set their access control setting to prevent JEDS from harvesting the objecting individual's information or mark the individual's record with a "do not publish" attribute to hide it within the JEDS White pages queries.

Coming in the future is a JEDS User Maintenance Portal (JUMP) that will allow DOD PKI authenticated individuals to submitted data inputs for inclusion into their individual entries in the JEDS directory database.

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.

This information is work related contract and identity information collected from their respective DoD Components, thus release-able under FOIA guidelines. Their DOD Components can mark individual records with "do not publish" attribute to hide it from JEDS White pages queries.

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.