PRIVACY IMPACT ASSESSMENT (PIA)

For the

Data Fabric User Directory
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	3232
☐	**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

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 Data Fabric User Directory 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.

The Data Fabric system centralizes command and control information, and provides consistent and modern access methods acquiring that information, freeing C2 clients of today and the future from the need to access many discrete interfaces in order to obtain this data.

This system requires users to be authenticated, and authorized, prior to allowing data access, and it is for the purpose of authentication that the Data Fabric system requires user data to be kept locally.

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

User information kept in the Data Fabric LDAP includes information available from the IdMI interface, which includes data from the Defense Manpower Data Center (DMDC) system, which is information considered PII (FASC-N, DoD ID Number, etc).

The Data Fabric LDAP is an instance of OpenLDAP, configured to achieve appropriate access control security and limit the risks associated with storage of this PII. The OpenLDAP configuration package used by the Data Fabric is accredited by DISA SE&I for this purpose.

Additionally, the Data Fabric system does not plan on disseminating user information: it only plans to use the collected user information to enable authentication to the system (through SIPRnet hard token, details of which are provided by DMDC). This limits the exposure of the PII data.

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. NA, PII will not be shared, used for authentication only and is encrypted.

☒ **Other DoD Components.**

Specify. NA, PII will not be shared, used for authentication only and is encrypted.

☒ **Other Federal Agencies.**

Specify. NA, PII will not be shared, used for authentication only and is encrypted.

☒ **State and Local Agencies.**

Specify. NA, PII will not be shared, used for authentication only and is encrypted.

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

Specify. NA, PII will not be shared, used for authentication only and is encrypted.

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

Specify. NA, PII will not be shared, used for authentication only and is encrypted.

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.

Individuals using the system are either sourced from DMDC (in which case their objections to the use of their data can be made directly to DMDC) or are added piecemeal to the system in extraordinary cases (in which case they are consenting to use the system). Note that in the latter case, individuals are only supplying credential information (username/password information) in order to gain system access: fields provided from DMDC that are considered PII are not collected for such users.

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.

Individuals using the system are sourced from DMDC (in which case they can refuse to give consent to DMDC).

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.	Individuals are never asked to provide PII data to the Data Fabric system, as that data is automatically sourced from DMDC (via IdMI).

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.