PRIVACY IMPACT ASSESSMENT (PIA)

For the

Personnel Security (PERSEC)
Defense Logistics Agency

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	
☐	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: S153.20 (Automated Listing of Eligibility and Clearances)

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 3206-0005

Enter Expiration Date 3/31/2013

☐ **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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; E.O. 10450, Security Requirements for Government Employment; E.O. 12958, Classified National Security Information; DoD Regulation 5200.2, DoD Personnel Security Program; and E.O. 9397 (SSN).

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.

PERSEC is a web application used by DLA personnel security specialists to maintain security clearance information on DLA civilian employees, military personnel, and contractors assigned to DLA. It is primarily a case management system used to supplement the Joint Personnel Adjudications System (JPAS) and to access information through database feeds. While JPAS is used to determine clearance eligibility, PERSEC is used to track security investigation status and generate summary reports.

Personal Information Collection are: Name, Address, family members, Dates of Birth, Place of Birth, Mother's Maiden name, Citizenship status, and SSN.

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

Some privacy risks associated with PII collection were identified for PERSEC: (1) unauthorized access (compromise of data resulting in identity theft would be devastating and threaten DLA's reputation), (2) unauthorized disclosure can result in identity theft.

In response to the risks that unauthorized access to the PII data contained in PERSEC records, PERSEC is protected under the defense-in-depth approach being taken by DLA Headquarters Information Technology System (HQITS) to protect this data. The PERSEC application is on the DLA HQITS network. Physical (PERSEC data is stored on an accredited, secured server within DLA HQ), technical (common access card (CAC) and personal identification number (PIN) are required for PERSEC access), and procedural (role-based access controls restrict access to PERSEC based on job category and permissions) safeguards are employed in series to ensure only those personnel that have a validated need-to-know can access this sensitive information. Individuals requiring access to the system will be processed IAW DoD 5200.1R and DLA Personnel Security Policies. The system administrators will ensure that only cleared personnel will have access to PERSEC as required according to their assigned duties. Cleared personnel verification documentation is held at the DLA system access control office.

In response to the risk presented by unauthorized disclosure of data within PERSEC records system users are made aware of restrictions on secondary uses of the data by initial and refresher Privacy Act and Information Assurance annual training that all DLA employees are required to take. Training emphasizes the importance of protecting personal information from loss, theft, and compromise. In addition, data sharing occurs only among individuals authorized access to the system of records as stated in the governing Privacy Act system notice. Dangers are prevented in providing notice of the collection or allowing an individual to object/consent. . Therefore, individuals are given this opportunity at times of notice publication and data collection. Afterwards, individuals may raise objections if new threats are perceived.

Other safeguards in place are the access to PERSEC is centrally controlled by designated DI personnel at DLA Headquarters. Designated DI personnel assigned as administrators review and approve all PERSEC users. New users request accounts via the administrator by using a digitally signed and encrypted e-mail. Administrators review and approve/disapprove requests and users will be notified accordingly. PERSEC users will be restricted to managing records to their respective organizations but will be able to view all records in the system. DI administrators will have access (view and edit) to all records.

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. DLA Security Managers, and Personnel Security Specialists

☐ **Other DoD Components.**

Specify.

☐ **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.

The forms used to collect the data contain Privacy Act Statements as required by 5 U.S.C. 522a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary; and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the DLA HQ Privacy Act office at any time.

(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.

The forms used to collect the data contain Privacy Act Statements as required by 5 U.S.C. 522a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary; and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the DLA HQ Privacy Act office at any time.

(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.

The individuals are provided the following: SF Form(s) 85, 85P, 86, 86A, 86C (forms), or access to the Electronic Questionnaires for Investigations Processing (E-QUIP), an electronic database containing a compilation of the forms. All forms or E-QUIP provide privacy act statements to the individuals informing them that the information collection is voluntary and the consequences of choosing not to participate in the information collection. Please refer to specific form(s) for Privacy Act Statement(s).

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.