PRIVACY IMPACT ASSESSMENT (PIA)

For the

Automation of DLA EEO Complaint Files
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

EEOC/GOVT-1 EEO in the Federal Government Complaint and A

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.

42 U.S.C. 2000e-16(b) and (c); 29 U.S.C. 204(f) and 206(d); 29 U.S.C. 633(A); 29 U.S.C. 791; Reorg. Plan No. 1 of 1978, 43 fr 19607 (May 9, 1978); E.O. 12106, 44 FR 1053 (January 3, 1979).

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 is to digitize Defense Logistics Agency (DLA) Equal Employment Office (EEO) records to provide protection against threats to data integrity, and maintain backup plans. The backup strategy is implemented through Defense Logistics Agency Document Services scanning all the material and transferring all data electronically to the DLA EEO offices which can be accessed through the internet with a Common Access Card (CAC). Records will be accessible only by EEO. These records are stored in DACS.

The database relies on these personal identifiers: Individual name, home address, home telephone number, work telephone number, and information about the alleged discrimination claim (basis[es]), issue[s] and requested relief).

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

The risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards as described below.

Administrative: Users, including individuals responsible for system maintenance, receive initial and periodic refresher Privacy Act and Information Assurance training. Users are warned through logon procedures of the conditions associated with access and the consequences of Improper activities. Users are required to accept those conditions/consequences before logon completes.

Physical: The data resides on a computer system that is connected to the World Wide Web. Central Processing Units are located in a secure computer facility with strong physical access controls required for entry. Within the secure facility, central processing units are kept in locked or controlled access areas. Electronic records are backed up periodically. Areas housing central processing units, servers, and work stations are configured with a fire suppression system. Should the system fall, the lost data could be constructed from the back-up records, paper files, and input sources.

Technical: The electronic records are deployed on accredited systems with access restricted via CAC. The Web-based files are encrypted in accordance with approved information assurance protocols. The system uses built-in virus detection software with notifications to alert administrator of new viruses. Computer terminals are password controlled with system-generated forced password change protocols. Computer screens automatically lock after a preset period of inactivity with reentry controlled by password. Systems manually locked by the user also require password for reentry. Shutdown compliance is periodically checked.

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.

Defense Logistics Agency Document Services, DLA EEO with a need to know

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.

☒ ☐

All personal data collected is voluntarily given by the complainant. The pre-complaint and formal complaint forms that collect personal data contain a Privacy Act Statement. It allows the individual to make an informed decision about providing the data or participating in the program. The Privacy Act Statement Disclosure advises that participation is voluntary. However, if the individual does not furnish the information requested, processing the complaint may be delayed or impaired.

(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.

☒ ☐

PRIVACY ACT STATEMENT

Authority: The Rehabilitation Act of 1973, a amended; 29 U.S.C. 791, Employment of Individuals with Disabilities; E.O. 13163, Increasing the Opportunity for Individuals with Disabilities to be Employed in the Federal Government; and E.O. 13164, Requiring Federal Agencies to Establish Procedures to Facilitate the Provision of Reasonable Accommodation.

Purposes(s): Information is being collected and maintained for the purpose of considering, deciding, and implementing requests for reasonable accommodation made by DLA employees and applicants with disabilities.

Routine uses: In addition to DoD "Blanket Routine Uses", records may be provided to first aid and safety

personnel for emergency treatment, Department of Labor for workers compensation claims, Federal Government officials investigating compliance with The Rehabilitation Act of 1973, as amended, and the U.S. Equal Employment Opportunity Commission (EEOC). The DoD "Blanket Routine Uses" may be found at http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

Disclosure - Voluntary; however, failure to provide this information may delay or impede your Reasonable Accommodation Request.

Rules of use: Rules for collecting, using, retaining, and safeguarding this information are contained in S330.50, entitled "Reasonable Accommodation Request Records" available at http://dpcld.defense.gov/Privacy/SORNs.aspx

(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: The Rehabilitation Act of 1973, a amended; 29 U.S.C. 791, Employment of Individuals with Disabilities; E.O. 13163, Increasing the Opportunity for Individuals with Disabilities to be Employed in the Federal Government; and E.O. 13164, Requiring Federal Agencies to Establish Procedures to Facilitate the Provision of Reasonable Accommodation.

Purposes(s): Information is being collected and maintained for the purpose of considering, deciding, and implementing requests for reasonable accommodation made by DLA employees and applicants with disabilities.

Routine uses: In addition to DoD "Blanket Routine Uses", records may be provided to first aid and safety personnel for emergency treatment, Department of Labor for workers compensation claims, Federal Government officials investigating compliance with The Rehabilitation Act of 1973, as amended, and the U.S. Equal Employment Opportunity Commission (EEOC). The DoD "Blanket Routine Uses" may be found at http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

Disclosure - Voluntary; however, failure to provide this information may delay or impede your Reasonable Accommodation Request.

Rules of use: Rules for collecting, using, retaining, and safeguarding this information are contained in S330.50, entitled "Reasonable Accommodation Request Records" available at http://dpcld.defense.gov/Privacy/SORNs.aspx

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.