PRIVACY IMPACT ASSESSMENT (PIA)

For the

Internet Complaints Management System (iComplaints)
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

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 Exempt Collections per DoD 8910.1-M

☒ **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); Exec. Order No. 12106, 44 FR 1053 (Jan. 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.

MicroPact Engineering's iComplaints database tool allows DLA to electronically manage EEO complaints Agency-wide, and specifically track and report on field EEO complaints. The system provides congressionally mandated reports with greater accuracy and reduced effort. The tool allows DLA to comply with reporting requirements of the Notification and Federal Employment Anti-Discrimination and Retaliation Act of 2001 (No FEAR) signed into law in May 2002. The tool captures events and case details in the Federal EEO complaints process from the pre-complaint stage through the appeal and civil action stages IAW Title 29 of the U.S. Code of Federal Regulations (CFR), Part 1614, Federal Sector Equal Employment Opportunity. Records are used to generate statistical reports to evaluate/analyze the status, trends, and effectiveness of the EEO complaint process in DLA. Reports generated do not contain and personally identifiable information. However, personal information collected includes the individual's name, home address, personal number, personal e-mail, biometrics, pregnancy details, and information regarding the alleged discrimination claim.

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

Identity theft, blackmail and public embarrassment are some of the risk associated with the personally identifiable information (PII) and EEO complaint information collected by this system. These risks are addressed by the use of strong passwords or smart cards used to access the system, Advanced Encryption Standards (AES), encryption of data at rest and in transit, and finally role-based security, which ensures that access to the information in the system is limited by job requirement and authorization to view the 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. Data may be viewed by or shared with employees assigned to DLA EEO offices such as EEO Managers, EEO Specialists, and EEO Assistants, for the purpose of performing the Agency's complaint processing functions under 29 CFR Part 1614, Federal Sector Equal Employment Opportunity.

☐ **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. Information collected may be shared through system-generated reports with EEOC Administrative judges, Federal judges, attorneys, and others involved with an EEO case. Complaint information is shared with Complainant's attorney as appropriate. Case files are not stored in this IT tool. With a written request of the complainant, information from the database may be shared with congressional offices or attorneys retained by the complainant. Data from this tool may be shared with contracted counselors, employers of contract investigators and witnesses, as appropriate, to carry out the Agency's complaint processing responsibilities under 29 CFR Part 1614, Federal Sector Equal Employment Opportunity.

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 provided by the complainant. The pre-complaint and formal complaint forms that collect the personal data that is captured by the system contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data or participating in the program.

(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.

As described above, all personal data collected is voluntarily provided by the complainant. The pre-complaint and formal complaint forms that collect the personal data that is captured by the system contain a Privacy Act Statement stating that failure to complete all portions of the form(s) may lead to dismissal of the complaint on the basis of inadequate data on which to determine if complaint is acceptable for processing.

(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 Statements are provided to individuals at the time the data is collected.

AUTHORITY: 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).

PRINCIPAL PURPOSE(S): Information is collected in order to counsel, investigate and adjudicate complaints of employment discrimination and related appeals brought by applicants and current and former federal employees against federal employers.

ROUTINE USE(S): To disclose information to another federal agency, to a court, or to a party in litigation before a court or in an administrative proceeding being conducted by a federal agency when the government is a party to the judicial or administrative proceeding. To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual. To disclose to an authorized appeal grievance examiner, formal complaints examiner, administrative judge, equal employment opportunity investigator, arbitrator or other duly authorized official engaged in investigation or settlement of a grievance, complaint or appeal filed by an employee. To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding. For a complete list of routine uses, visit http://dpclo.defense.gov/privacy/SORNs/govt/EEOCGOVT-1.html.

DISCLOSURE: Voluntary; however, failure to complete all portions of this form may lead to dismissal of complaint on the basis of inadequate data on which to determine if complaint is acceptable for processing.

RULES OF USE: Rules for collecting, using, retaining, and safeguarding this information are contained in Privacy Act System Notice EEOC/Govt-1, entitled "Equal Employment Opportunity in the Federal Government Complaint and Appeal Records" available at http://dpclo.defense.gov/privacy/SORNs/govt/EEOCGOVT-1.html.

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.