PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Logistics Agency Criminal Incident Reporting System (DCIRS)
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	14343
☐	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: S500.20

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 Pending

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 Omnibus Crime Control Act of 1994; Section 21, Internal Security Act of 1950 (Pub. L. 831, 81st Congress); DOD Directive 5105.22, Defense Logistics Agency (32 CFR part 359); DOD Directive 5105.42, Defense Security Service (32 CFR part 361); DOD Directive 7730.47, Defense Incident-Based Reporting System; DOD Instruction 2030.8, Trade Security Controls on DOD Excess and Surplus Personal Property; DOD Instruction 5240.4, Reporting of Counterintelligence and Criminal Violations; DOD Instruction 5505.2, Criminal Investigations of Fraud Offenses; 28 U.S.C. 534, Uniform Federal Crime Reporting Act; 18 U.S.C. 922, Brady Handgun Violence Prevention Act of 1994; 42 U.S.C. 10601, Victim Rights and Restitution Act of 1990; 10 U.S.C. 1562, Database on Domestic Violence Incidents; 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.

Information in this system is used by DLA Office of Investigations, DLA Offices of Public Safety, and the DLA Office of General Counsel personnel to monitor progress of cases and to develop non-personal statistical data on crime and criminal investigative support for the future. DLA General Counsel also uses data to review cases, determine proper legal action, and coordinate on all available remedies. Information is released to DLA managers who use the information to determine actions required to correct the causes of loss and to take appropriate action against DLA employees or contractors in cases of their involvement. Records are also used by DLA to monitor the progress of investigations, identify crime conducive conditions, and prepare crime vulnerability assessments/statistics.

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

The risks to the collection, use, and sharing of the information in identifiable form is alleviated by collecting and maintaining the data in a secure and accredited system. All system users are made aware of restrictions on secondary uses of the data by initial and refresher Privacy Act and Information Assurance training. In addition, data sharing occurs only among individuals authorized access to the system of records as stated in the governing Privacy Act system notice. Computer terminals with DCIRS are password controlled with system-generated, forced password-change protocols (every 90 days) and are also equipped with "smart card" technology that requires the insertion of an embedded identification card and entry of a personal identification number (PIN).

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. Commander of DLA Headquarters Special Staff; DLA Office of General Counsel; DLA Personnel Security Section; and DLA Office of Public Safety.

☒ **Other DoD Components.**

Specify. Defense Criminal Investigative Service; Air Force Office of Special Investigations; Defense Intelligence Service; Naval Criminal Investigative Service; and the DOD Inspector General

☒ **Other Federal Agencies.**

Specify. Federal agencies having jurisdiction over or investigative interest in the investigation.

☒ **State and Local Agencies.**

Specify. State and local agencies having jurisdiction over or investigative interest in the investigation.

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

Specify. To DLA contractors or vendors when the investigation pertains to a person they

employ or to a product or service they provide to DOD when disclosure is necessary to accomplish or support corrective action.

☐ **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 voluntary.

(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.

Verbally or in writing.

(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: Section 21, Internal Security Act of 1950 (Public Law 81-831).

Principal purpose: Records are used in connection with an incident, accident, or suspected violation under investigation, regardless of the individual's relationship to the investigation.

Routine uses: Information is used by Investigations Division, DLA Accountability Office and the DLA Office of General Counsel personnel to monitor progress of cases and to develop non-personnel statistical data on crime and criminal investigative support for the future. This information may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.

Disclosure: Disclosure is voluntary.

Rules of Use: Rules for collecting, using, retaining, and safeguarding this information are contained in the DLA Privacy Act System of Records Notice S500.20, entitled "Defense Logistics Agency Criminal Incident Reporting System Records" available at http://privacy.defense.gov/notices/dla/

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.