PRIVACY IMPACT ASSESSMENT (PIA)

For the

DLA PoliceCenter (POLC)
Defense Logistics Agency - DLA Installation Support

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	Pending in J62 (Feb 2013)
☐	**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 S500.30 - Incident Investigation/Police Inquiry Files, S500.40 (D

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.

Police Center's collection is covered by several legal authorities from five separate Privacy Act Systems of Records. In each system, the legal authorities for collection and maintenance of the system is listed.

Those systems include:

1. S500.30 (Incident Investigation/Police Inquiry Files)
2. S500.40 (DLA Security Force and Staff Records)
3. S500.41 (Vehicle/Traffic Incident Files)
4. S500.42 (Seizure and Disposition of Property Records)
5. S500.43 (Firearms Registration Records)

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.

This system combines several existing functions of the DLA police force mission. Police Center will serve as an enterprise wide system for the collection and storage of police records. This system will track criminal incident data at HQ and the major DLA field sites through information sharing to assist in crime prevention strategies, crime trends, and criminal activities. This information will enhance police capabilities and better protect the DLA installations. Additionally this information will give Headquarters personnel oversight on criminal activity for developing Antiterrorism/Physical Security prevention methods, thus better protecting DLA assets and personnel. Information gathered by Police officers will only be for official police matters and will only be gathered for record keeping only.
PII collected will include: names, drivers license numbers, personal addresses, telephone numbers, social security numbers, date of birth, place of birth, security clearance, education data, law enforcement and background (criminal background). This information will be protected in accordance with Executives Orders, DoD Directives and DLA Policies.

(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 Police Center: (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 PoliceCenter records, this new system will be protected by DLA policies on Information Assurance. All infrastructure supporting PoliceCenter will have all applicable Security Technical Implementation Guides (STIGs), checklists, and vulnerability scans applied. Additionally only authorized DLA Police Officers and DS-S Security and Emergency Services Personnel will be allowed access. All personnel will be vetted by HQ Installation Support prior to access being granted. Access will be solely via CAC authentication.

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 Intelligence (DI) (as needed) and DLA General Counsel.

☒ **Other DoD Components.**

Specify. Office of Inspector General (OIG), U.S. Military Law Enforcement Officials (as needed for active cases), Commanders of individuals (as needed), and appropiate DoD legal agencies pertaining to the police matter.

☒ **Other Federal Agencies.**

Specify. Federal Bureau of Investigations (FBI) as needed, Department of Homeland Security (DHS) as needed, other Federal Agencies as needed in criminal matters, and legal officials when requested. U.S. Department of Labor (worker compensation claims)

☒ **State and Local Agencies.**

Any State or Local Police Department responding to a police matter or

Specify. investigating a police matter affecting DLA assests or resources. Local Hospital or medical facilities (treatment of accidental injury).

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

Specify. Interact Company is the contractor awarded this contract and will have access to the information. The following mandatory FAR Clauses have been incorporated into the Police Center Contract:

FAR 52.224-1, Privacy Act Notification, FAR 52.224-2, Privacy Act, and 52.239-1, Privacy and Security Safeguards.
Additionally, the following Privacy Guidance is incorporated: FAR 39.105 Privacy -- that states the rules of conduct that the contractor and contractor's employees shall be required to follow. FAR 39.105, Privacy, states that contracts for information technology shall address protection of privacy in accordance with the Privacy Act, Title 5 United States Code section 552a, and FAR Part 24. In addition, contracts for the design, development, or operation of a system of records using commercial information technology services or information technology support services must include Agency rules of conduct that the contractor and the contractor's employees shall be required to follow. The Department of Defense rules of conduct are defined at 32 CFR Section 310.8. Per 32 CFR Section 310.8(a)(3), the "Privacy POC" to contact in the event of a breach of PII are both the DLA contracting officer responsible for this contract and the DLA Network Operations and Security Center (NOSC) at 1-877-352-6366.

☐ **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.

Individuals may object to the collection of their PII, however their objection would lead to the inability to provide police-related services or benefits such as vehicle traffic accidents occurring on the installlation.

(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.

Individuals may object to the collection of their PII, however their objection would lead to the inability to provide police-related services and/or benefits such as vehicle traffic accidents occurring on the installlation.

(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.	PII is gathered directly from the individuals. Officers will gather PII on the respective forms relating to the police matters. For instance, incidents involving vehicle traffic accidents would require a completion of DL 1625 (Security Force Traffic Accident Report), incidents involving criminal activity may require the completion of DL 1745 (Consent to Search), etc. which include a Privacy Act Statement given to the individuals.

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.