



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Police Cross Index (PCI)

Defense Logistics Agency (DLA)

### **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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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

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**

OMB number request submitted 1/21/2011

**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.

The Police Cross Index is used to enter and view details related to individuals, investigations, and incidents.

Personal information collected by the system includes: Name; Gender; Race/Ethnicity; Birth Date; Mailing/ Home Address; and Biometrics (fingerprints).

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

Risk exposure of individual's private and personal information. The risks are minimized by physical, technical, and administrative controls. Data is available to only those whose job performances require access. System access is controlled by use of smart cards and role-based security which ensures 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.

**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.

Incident report forms are filled out by DLA Installation Support Personnel (security personnel), DLA Accountability Office Investigations Division personnel, and Defense Criminal Investigation Service personnel. At the time of initial collection, a Privacy Act Statement may be provided to the subject individual. The information collected is used for the specific purposes of site security pursuant to 32 CFR 1292.5, Security of DLA Activities and Resources, and to track emergency services and day-to-day security functions.

(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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

If the subject individual agrees to provide information, pursuant to the Privacy Act systems of records notice published in the Federal Register on April 14, 2010 (page 19377) and the Privacy Act Exemption Rule published in the Federal Register on October 29, 2009 (page 55781), the individual does not have the opportunity to consent to specific uses of their PII.

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.

DLA forms are presented to individuals containing a Privacy Act Statement. Form revision is pending with estimated completion date of September 15, 2011.

**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.