

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Police Center (POLC)

2. DOD COMPONENT NAME:

Defense Logistics Agency

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- | | |
|--|--|
| <input type="checkbox"/> From members of the general public | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

b. The PII is in a: (Check one)

- | | |
|--|---|
| <input type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input checked="" type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> Significantly Modified DoD Information System | |

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

Police Center will serve as an enterprise-wide system for the collection and storage of police records. This system will provide all five DLA police agencies information sharing capability for crime prevention strategies, crime trends, and criminal activities. This information will enhance police capabilities and better protect their installations. Additionally this information will give Headquarters personnel oversight on criminal activity for developing Anti-terrorism/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 be gathered for record keeping only. PII collected will be protected in accordance with the law, Executive Orders, DoD Directives, and DLA Policies.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

PII is gathered to properly verify and identify personnel involved in a police matters, conduct law enforcement record checks, and generate law enforcement referrals/leads. Additionally, contractor, and vendor personnel, delivery personnel coming onto the DLA Installations for activities who may be involved in auto-accidents, criminal activity, damaged, or lost property may have PII collected for police reports.

e. Do individuals have the opportunity to object to the collection of their PII? Yes No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

PII must be gathered to complete Police Reports and conduct investigations for any instance identified as a police/security related matter or incident. If PII is not obtained and recorded the identification of suspects, victims, or witnesses will be severely affected and potentially damaging to the prosecution for criminal offenses, suspicious activity, or terrorist threats/activities affecting DLA/DoD installations and activities. References include, but are not limited to, DOD Instruction 5525.19, DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Databases (TSDB) and Privacy Act of 1974, Conditions of Disclosure to Third Parties, Section 7. 5 U.S.C. § 552a(b)(7) (law enforcement request) and 8. 5 U.S.C. § 552a(b)(8) (health or safety of an individual).

f. 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.

PII must be gathered to complete Police Reports and conduct investigations for any instance identified as a police/security related matter or incident. Permitting individuals to select or consent to specific uses of their PII limits effectiveness of law enforcement and security personnel in investigations into criminal, suspicious, or terrorist activities. References include, but are not limited to, DOD Instruction 5525.19, DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist

Screening Databases (TSDB) and Privacy Act of 1974, Conditions of Disclosure to Third Parties, Section 7. 5 U.S.C. § 552a(b)(7) (law enforcement request) and 8. 5 U.S.C. § 552a(b)(8) (health or safety of an individual).

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

Privacy Act Statement Privacy Advisory Not Applicable

PRIVACY ACT STATEMENT

Authority: 5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 303(b), Oath to Witnesses; 10 U.S.C. 133, Under Secretary of Defense for Acquisition and Technology; and E.O. 9397 (SSN), as amended. 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; Section 21 of the Internal Security Act of 1950 (50 U.S.C. 797); 18 U.S.C. 499, Military, Naval, or Official Passes; 18 U.S.C. 701, Official Badges, Identification Cards, Other Insignia; 18 U.S.C. 716, Police Badges; National Highway Safety Act of 1966 (23 U.S.C. 401, Highway Safety, et seq.); DOD Instruction 5200.8, Security of Military Installations and Resources; 10 U.S.C. 1580, Emergency Essential Personnel, designation; DOD Directive 5210.56, Use of Deadly Force and the Carrying of Firearms by DOD Personnel Engaged in Law Enforcement and Security Duties; 10 U.S.C. 1585, Carrying of Firearms; 10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; 10 U.S.C. 1593, Uniform allowance: civilian employees; Section 21 of the Internal Security Act 1950 (50 U.S.C. 797, et seq.); DOD Instruction 5200.8, Security of DOD Installations and Resources; DOD Instruction 6055.17, Installation Emergency Management Program; CJCSI 3121.01B, Standing Rules of Engagement/Standing rules for the Use of Force for US Forces; DOD Directive 5105.22, Defense Logistics Agency; and E.O. 9397 (SSN) as amended.

Purpose: Information is collected to serve as an enterprise wide system for the collection and storage of police records. This system will track criminal and non-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. The information collected also assists DLA's oversight of criminal activity for developing Antiterrorism/Physical Security prevention methods.

Routine Uses: In addition to the DoD "Blanket Routine Uses" which apply to this system of records, the records may be released: To Federal, state, and local agencies that administer programs or employ individuals involved in an incident or inquiry; To medical and emergency personnel to make medical and safety determinations about individuals involved in accidents; And to the Department of Labor, Office of Workers' Compensation for the purpose of processing workers' compensation claims.

Disclosure: Voluntary; however, failure to provide the requested data may result in the inability to provide police-related services or benefits.

Rules of Use: Rules for collecting, using, retaining and safeguarding this information are contained in Defense Logistics Agency Notices, S500.30, "Incident Investigation/Police Inquiry Files", S500.40, "DLA Security Force and Staff Records," S500.41, "Vehicle/Traffic Incident Files," S500.42, "Seizure and Disposition of Property Records," and S500.43, "Firearms Registration Records" located at: <http://dpcl.d.defense.gov/Privacy/SORNSIndex/DOD-Component-Notices/DLA-Article-List/>

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

Within the DoD Component

Specify.

Office of Inspector General (OIG), DLA Intelligence (DI), DLA General Counsel (DG)

Other DoD Components

Specify.

U.S. Military Law Enforcement Officials including Army Criminal Investigation Services (CID), Navy Criminal Investigation Services (NCIS), Air Force Criminal Investigation Services, Coast Guard Criminal Investigation Services, (as needed for active cases), military Commanders of individuals (as needed), Judge Advocate General (JAG), and appropriate legal agencies with DOD pertaining to code of criminal justice enforcement police matter.

Other Federal Agencies

Specify.

Federal Bureau of Investigations (FBI) as needed, Department of Homeland Security (DHS) as needed, any other Federal Agencies, as needed, who are responsible for code of criminal justice, anti-terrorism, law enforcement or prosecution of criminal justice matters, and legal officials when requested through appropriate channels.

State and Local Agencies

Specify.

Any State or Local Police Department responding to a police matter or investigating a police matter affecting DLA assets or resources.

Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)

Specify.

RightDirection Technology Solutions, Inc. (RDTS) is the contractor awarded this contract and working with the Commercial-Off-The-Shelf (COTS) vendor Caliber Public Safety for the InterAct Records Management System (RMS) and will have access to the information input into the system. The Contractor may have access to information covered under the Privacy Act of 1974, and if so, the Contractor shall comply with all applicable safeguarding and handling requirements associated with Privacy Act data (www.usdoj.gov). Paragraph 5.6. of the contract states: Performance of this contract may require the Contractor and, perhaps, sub-contractor to access data and information proprietary to the Government agency or of such a nature that its dissemination or use, other than in performance of this Performance Based Work Statement (PWS) would be adverse to the interest of the Government or others. The Contractor shall not divulge or release data or information developed or obtained in performance of this PWS. The Contractor shall not use, disclose, or reproduce proprietary data, which bears a restrictive legend, other than as required in the performance of this PWS. The limitations above do not apply to data or information made public by the Government. Further, this provision does not preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner that provides for greater rights to the Contractor. All products, partial products, and associated work papers produced in the course of fulfilling orders placed under this contract will be considered the property of the DLA. Modifications will be made to the contract to reflect the requirements set forth in FAR 24.104, and DoDI 8500.2, and PROCLTR 2012-05 (for the inclusion of FAR 52.224-1 and FAR 52.224-2, and DFARS Subparts 239.71 and 239.72)

Other (e.g., commercial providers, colleges).

Specify.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

Individuals

Databases

Existing DoD Information Systems

Commercial Systems

Other Federal Information Systems

PII will be gathered directly from the individual (witness, suspect, subject, victim). On occasion, PII maybe gathered over a telephone where face-to-face contact is not possible. PII may also be obtained from both state and national Criminal Justice Information Systems (CJIS) including the FBI maintained National Criminal Information Computer (NCIC); state criminal information systems for Virginia, Pennsylvania, California, and Ohio; and department of motor vehicle information systems for Virginia, Pennsylvania, California, and Ohio. This information is queried through the systems listed by the officer or dispatcher and then entered into the RMS police report, as needed for investigative purposes.

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

E-mail

Official Form (Enter Form Number(s) in the box below)

Face-to-Face Contact

Paper

Fax

Telephone Interview

Information Sharing - System to System

Website/E-Form

Other (If Other, enter the information in the box below)

DLA Form 635

k. 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 must be consistent.

Yes No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcltd.defense.gov/Privacy/SORNS/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

I. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

6055.5: Criminal Incident/Investigations Files - When Entered into DCIRS. Reports of investigation; messages; statements of witnesses, subject and victims; photographs; laboratory reports; data collection reports; and other related papers. Records pertain to civilian and military personnel of DLA, contractor employees and other persons who committed or are suspected of having committed a felony or misdemeanor on DLA controlled activities or facilities; or outside of those areas in cases where DLA is or may be a party of interest. (Reports of Investigation, Response to Leads, Reports of Corrective Action, Commander or Director's Reports of Corrective Action, Reports of preliminary Inquiry, Reports of Referral, and Police Incident Reports). TEMPORARY. Cutoff at end of Event - Destroy/Erase 25 years after completion.

6055.5.01: Criminal Incident/Investigation File - When Not Entered into DCIRS. Reports of investigation; messages; statements of witnesses, subject and victims; photographs; laboratory reports; data collection reports; and other related papers. Records pertain to civilian and military personnel of DLA, contractor employees and other persons who committed or are suspected of having committed a felony or misdemeanor on DLA controlled activities or facilities; or outside of those areas in cases where DLA is or may be a party of interest. (Reports of Investigation, Response to Leads, Reports of Corrective Action, Commander or Director's Reports of Corrective Action, Reports of Preliminary Inquiry, Reports of Referral, Police Incident Reports). TEMPORARY. Cutoff at end of Event. - Destroy/Erase 10 years after completion.

6055.9: Analysis of Criminal Offenses and Trends - Summaries, charts, graphs and statistical data reflecting trends in crime. TEMPORARY. Cutoff at end of Event. - Destroy 3 years after supersessions or obsolescence.

6055.15: Motor Vehicle Registration - Documents and records relating to permanent registration of private vehicles to include commercial vehicles. TEMPORARY. Cutoff at end of Event. - Destroy upon normal expiration or supersession of registration or 3 years after revocation of registration.

6055.16: Motor Vehicle Liability Insurance - Documents pertaining to requirements for motor vehicle liability insurance coverage, accepted, and accredited insurers, solicitation and sale, suspension or withdrawal of solicitation or accreditation privileges, reports, notices, certificates, and other related documents. TEMPORARY. Cutoff at end of Event. - Destroy after 1 year, or when superseded or no longer needed, whichever is later except that documents pertaining to suspension or withdrawal actions initiated by DLA activities will be retained and destroyed after 3 years.

6055.17: Vehicle Accident Investigation - Reports, sketches, and related papers concerning accident investigations. TEMPORARY. Cutoff at end of CY. - Destroy after 2 years.

6055.18: Traffic Violations - Documents relating to traffic tickets for moving and nonmoving violations, withdrawal of driver permits, and related papers. TEMPORARY. Cutoff at end of Event. - Destroy after 2 years.

6055.19: Seizure and Disposition of Property - Documents pertaining to acquisition and disposition of contraband and physical evidence. TEMPORARY. Cutoff at end of Event. - Destroy 3 years after final action, except criminal cases in which retention and disposition will be as series 6055.5, Criminal Incident/Investigations File.

6055.20: Firearms Registration - Documents relating to registration of privately owned weapons and firearms. TEMPORARY. Cutoff after cancellation of registration or departure of registrant from jurisdiction of registering activity. - Destroy 1 year after cancellation of registration or departure of registrant from jurisdiction of the registering activity.

6055.21: Loss and Recovery of Firearms and Ammunition: HQ DLA Command Security - Documents and reports relating to the loss and recovery of firearms and ammunition including equipment designed to increase the efficiency or destructiveness of firearms. Includes reports made by HQ DLA to the National Crime Information Center (NCIC). TEMPORARY. - Destroy after 10 years.

6055.21.01: Loss and Recovery of Firearms and Ammunition: Other Offices - Documents and reports relating to the loss and recovery of firearms and ammunition including equipment designed to increase the efficiency or destructiveness of firearms. Includes reports made by HQ DLA to the National Crime Information Center (NCIC). TEMPORARY. - Destroy after 3 years.

6055.27 Protective Communications. Documents relating to use, design, installation, maintenance, and security of communication nets used by protective services forces. Temporary. Cutoff at end of CY. Retain in CFA. Destroy after 3 years or when the communications net is removed, whichever is later.

6055.28 Police Force Records. Documents relating to operation and use of a police force; clearances, qualifications, training, examination, uniforms, and weapons of personnel; and order, supervision, records, and reports. Temporary. Cutoff at end of CY. Destroy after 1 year or when superseded or obsolete, as applicable.

6055.29 Police Blotter. DLA Form 1620 or similar records listing incidents and actions taken. May include ledger records of arrests, cars ticketed, and outside police contacts. Temporary. Cutoff at end of Event. Destroy 3 years after final entry.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
- (2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

S500.30 - 5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 303(b), Oath to Witnesses; 10 U.S.C. 133, Under Secretary of Defense for Acquisition and Technology; and E.O. 9397 (SSN), as amended.

S500.40- 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; Section 21 of the Internal Security Act of 1950 (50 U.S.C. 797); 18 U.S.C. 499, Military, Naval, or Official Passes; 18 U.S.C. 701, Official Badges, Identification Cards, Other Insignia; 18 U.S.C. 716, Police Badges; National Highway Safety Act of 1966 (23 U.S.C. 401, Highway Safety, et seq.); DOD Instruction 5200.8, Security of Military Installations and Resources; 10 U.S.C. 1580, Emergency Essential Personnel, designation; DOD Directive 5210.56, Use of Deadly Force and the Carrying of Firearms by DOD Personnel Engaged in Law Enforcement and Security Duties; CJCSI 3121.01B, Standing Rules of Engagement/Standing rules for the Use of Force for US Forces; 10 U.S.C. 1593, Uniform allowance: civilian employees; and E.O. 9397 (SSN).

S500.41 -10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; National Highway Safety Act of 1966 (23 U.S.C. 401, Highway Safety, et seq.); and E.O. 9397 (SSN).

S500.42 - Section 21 of the Internal Security Act 1950 (50 U.S.C. 797, et seq.); DOD Instruction 5200.8, Security of DOD Installations and Resources; DOD Directive 5105.22, Defense Logistics Agency; and E.O. 9397 (SSN).-

S500.43 - Section 21 of the Internal Security Act 1950 (50 U.S.C. 797, et seq.); DOD Instruction 5200.8, Security of DOD Installations and Resources; DOD Directive 5105.22, Defense Logistics Agency; and E.O. 9397 (SSN).

5 U.S.C. 301, Departmental Regulations, 5 U.S.C. 6122, Flexible schedules, agencies authorized to use; 5 U.S.C. 6125, Flexible schedules, time recording devices; 10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; 23 U.S.C. 401 et seq., National Highway Safety Act of 1966; E.O. 9397 (SSN); and E.O. 10450, Security Requirements for Government Employees.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 No Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
- (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."
- (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0704-0514, Expiration: 05/31/2017. The update for this registration has been sent to DLA representative for coordination and is pending final adjudication/update from DoD.