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:

Activity Management for Investigators and Analyst System

2. DOD COMPONENT NAME:

Defense Logistics Agency

3. PIA APPROVAL DATE:

09/16/22

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees
- [x] from both members of the general public and Federal employees
- [ ] Not Collected *(if checked proceed to Section 4)*

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

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] 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.

AMIAS is an Investigation and Audit management system used to manage case workloads within the Office of the Inspector General. The DLA OIG requires a Commercial Off The Shelf (COTS) system that manages activities for investigators and analysts, which are currently owned/utilized by the Federal Government and are adaptable to accommodate Investigative activities, Hotline activities, and Trade Security Controls (TSC) requirements, unique to the DLA OIG.

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)*

The PII in this system is obtained for, but not limited to, investigative, administrative, and audit purposes. The intended uses are verification, identification, authentication, data matching, mission related use, and administrative use.

e. Do individuals have the opportunity to object to the collection of their PII? [x] 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.

All personal data is collected voluntarily.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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.

Verbally or in writing.

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.)*

- [x] Privacy Act Statement
- [ ] Privacy Advisory
- [ ] Not Applicable

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. Information provided may be used to determine regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions. This information may be further disclosed to federal, state, local, and foreign governments, law enforcement agencies, prosecutors, courts, child protective services, and the Office of Personnel Management.

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/

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

[X]	Within the DoD Component	Specify.	D-Staff (Director/Vice Director/Staff); DLA Office of the Inspector General (DA); DLA Intelligence (DI); DLA General Counsel (DG); Safety & Occupational Health (DCS); Insider Threat Office
[X]	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Department of the Air Force; Department of the Army; Department of the Navy/U.S. Marine Corps; Defense Intelligence Agency; Defense Security Service; Office of Inspector General
[X]	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Federal agencies having jurisdiction over or investigative interest in the investigation.
[X]	State and Local Agencies	Specify.	County or City Governments; Tribal governments; State Government Agencies;
[X]	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.	Contractor: Cybermedia Technologies, Inc. (SP4709-17-D-0029 expiring 4/30/2023) FAR 52.224-3, Privacy Training (Jan 2017)
[X]	Other *(e.g., commercial providers, colleges).*	Specify.	To DLA contractors or vendors; when the investigation pertains to a person they employ or to a product or service they provide to accomplish or support corrective action.

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

- [X] Individuals
- [X] Databases
- [X] Existing DoD Information Systems
- [X] Commercial Systems
- [X] Other Federal Information Systems

Users of AMIAS collect information from individuals by using the following data systems via the web or via paper-based collections from subjects or witnesses: Accurint; Auto Track; Clear, Defense Central Index of Investigations; other DCIRS/AMIAS entries; GSA Excluded Parties List; Department of Commerce - Denied Persons List; Department of State Directorate; Defense Trade Controls; Duns & Bradstreet; Canadian Controlled Goods Directorate (for Canadians only); Department of Commerce Unverified List - Non-US Persons, National Crime Information Center, DLA DES OnGuard, DLA Human Resource Personnel Records, DLA Personnel Security Records; National Law Enforcement Telecommunications System; DLA Worker's Compensation files and other Law Enforcement databases as applicable; and public records available on the Internet.

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

- [X] E-mail
- [X] Official Form (*Enter Form Number(s) in the box below)*
- [X] In-Person Contact
- [X] Paper
- [X] Fax
- [X] Telephone Interview
- [X] Information Sharing - System to System
- [X] Website/E-Form
- [X] Other *(If Other, enter the information in the box below)*

DLA 1822, DD 2949, DLA Form 1624A, DLA Form 1745, DLA Form 1753, DLA Form 1622, DLA Form 1623

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.

- [X] Yes
- [ ] No

If "Yes," enter SORN System Identifier S500.20; S640.45

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.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.

l. 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. N1361-08-3; DAA=0361-2021-0021-0001; GRS 5.2, Item 020 (DAA-

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

(3) Retention Instructions.

8120.44 - DCIRS 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. Cutoff at the end of the Event. Destroy/erase 25 years after completion. N1-361-08-3
8120.44.01 - DCIRS Reports of Initiative, Crime Vulnerability Assessments, Reports of Post Sale Investigation, and Criminal Information Reports. Destroy/erase 10 years after completion. N1-361-08-3
8120.44.02 -DCIRS Trade Security Controls Assessment Records. Includes records related and not related to a specific transaction. Destroy/erase 6 years after the last transaction. N1-361-08-3
8120.44.03 - DCIRS Trade Security Controls Assessment Records. Reports of Outreach Destroy/erase 5 years after completion. N1-361-08-3
8120.44.04 -DCIRS Reports of Polygraph Examination. Temporary Records (Non-historical, as determined by the Defense Criminal Investigative Service (DCIS)). Destroy/erase 90 days following completion of the investigation. DAA-0361-2021-0021-0001
8120.44.05 - Series Approved for System Use Only. DCIRS Reports of Polygraph Examination. Attorney's Contract Fraud Files. Destroy/erase 6 years after completion. N1-361-08-3
8120.44.06 - End Use Certificate records. Used in the management of the property disposal programs to determine bidder eligibility to participate in the programs and ensure that property recipients comply with the terms of the sale regarding the end use of the property. They are also used to transfer DoD export controlled technical data to non-DoD entities. Destroy/erase 7 years after the bid award date. Sales records involving a violation of law or regulation are destroyed 15 years after case adjudication is completed. DAA-0361-2021-0021-0002
8120.44.07 - Input Source Records - Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. GRS 5.2, Item 020 (DAA-GRS-2017-0003-0002)
8122.44.08 - System Documentation. Data administration records and documentation relating to electronic records scheduled as temporary in the GRS or in NARA-approved agency schedule or any type of data administration records. Destroy 5 years after the project, activity, or transaction is completed or superseded. GRS 3.1, Item 051 (DAA-GRS-2013-0005-0003)

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 statue 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.

10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; 22 U.S.C. 2751-2799, Arms Export Control; 50 App. U.S.C. 2401 et seq., Export Administration; E.O. 12738 and E.O. 12981, Export Controls; 22 CFR 122, Registration of Manufacturers and Exporters; 15 CFR 762, Export Administration Regulations Recordkeeping; 41 CFR 101, Federal Property Management Regulations; 41 CFR 102, Federal Management Regulations; DoD Directive 2040.3, End Use Certificates (EUCS); DoD Instruction 2030.08, Implementation of Trade Security Controls (TSC) for Transfers of DoD U.S. Munitions List (USML) and Commerce Control List (CCL)

Personal Property to Parties Outside DoD Control; DoD Instruction 2040.02, International Transfers of Technology, Articles, and Services; DoD Instruction 4161.2, Management, Control and Disposal of Government Property in Possession of Contractors; DoD 4160.21-M, Defense Materiel Disposition Manual; DoD 4160.21-M-1, Defense Demilitarization Manual and E.O. 9397 (SSN), as amended.
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), as amended.

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.

0704-0382, collection End Use Certificate, expiring 5/31/2025