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:

Electronic Archive and Records Management System (EARMS)

2. DOD COMPONENT NAME:

Department of Defense Inspector General

3. PIA APPROVAL DATE:

3/28/2022

Mission Support Team, OCIO, Information Governance Division

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] 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.

EARMS is an archive system for the DoD OIG. EARMS is a system capable of automatically identifying electronic information as records while capturing and moving official copies from various locations into a single repository for litigation, investigative, and records management purposes. The system must be able to auto-capture semi-structured information (i.e., email), unstructured information (i.e., Microsoft Word documents), and structured information (i.e., information from databases). Also, the system must manage the full life-cycle of information including indexing, auto-categorizing, storing, managing-in-place, records declaration, archiving, migrating, deleting, transferring, auditing and exporting.

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)*

EARMS does not collect PII; however, PII may be transferred and maintained through the system as a regular course of business. DoD OIG collects PII to positively identify subjects, witnesses, and victims associated with a particular administrative or criminal investigation. This information is used by investigators to collaborate and coordinate investigative efforts. PII is reported in accordance with statutory and regulatory mandates to other DoD information systems, including DCII, DDEX, DIBRS, CRIMS, DCATSe, and other IT systems that are statutorily authorized where the information is used to positively identify persons involved in DoD OIG investigations.

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

Information is used and maintained in accordance with all applicable rules and regulations as required to carry out the mission of the DoD OIG under the IG Act.

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

Information is used and maintained in accordance with all applicable rules and regulations as required to carry out the mission of the DoD OIG under the IG Act.

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
- [x] Privacy Advisory
- [ ] Not Applicable

EARMS does not collect information directly from the individual. Information is maintained and used through system-to-system interfaces. Individuals who provide PII directly to the DoD OIG are informed either through a Privacy Act Statement or Advisory that the information is being collected in connection with official DoD OIG business, such as investigative or personnel management functions, and that the information collected may be used in furtherance of other official matters consistent with the purpose for which the information was collected.

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

[X] Within the DoD Component	Specify.	All DoD OIG components that require access for mission requirements.
[X] Other DoD Components	Specify.	Military Criminal Investigative Organizations, other members of the DoD Law Enforcement and Intelligence Communities, Defense Security Service, other DoD clearance and adjudicative facilities.
[X] Other Federal Agencies	Specify.	Federal law enforcement and auditing agencies, including the Federal Bureau of Investigation, Department of Homeland Security, and other Offices of Inspectors General.
[X] State and Local Agencies	Specify.	State and local law enforcement agencies.
[ ] 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.	
[ ] 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)*

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

EARMS does not collect PII; however, PII may be transferred and maintained through the system as a regular course of business. EARMS contains information from individuals interviewed during the course of an investigation. PII is collected from government and contractor information systems including personnel records, security files, contract files, pay records, and law enforcement information. PII is collected from commercial databases.

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

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

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 [X] 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://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.

A SORN is not required as it is not an ordinary course of business to retrieve information in EARMS by using a personal identifier.

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. Unscheduled

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

(3) Retention Instructions.

Do not destroy until the DoD OIG receives disposition authority. Unscheduled records are Federal records whose final disposition has not been approved by NARA on a SF 115, Request for Records Disposition Authority. Similar Federal records are approved for permanent retention.

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.

The authority to collect information in this system is derived from:
1) Public Law 95-452, The Inspector General Act of 1978;
2) Public Law 110-409, Inspector General Reform Act of 2008;
3) Public Law, 114-317, Inspector General Empowerment Act of 2016;
4) 5 USC § 4103, Establishment of Training Programs;
5) 10 USC § 113, Secretary of Defense;
6) 10 USC § 141, Inspector General;
7) 10 USC § 136, Under Secretary of Defense for Personnel and Readiness;
8) Public Law 111-352, Government Performance Results Act (GPRA) Modernization Act of 2010;
9) Comptroller General of the United States, Government Auditing Standards;
10) OMB Circular No. A-50, Audit Follow-up, revised September 29, 1982;
11) DoD Directive 5106.01, Inspector General of the Department of Defense (IG DoD);
12) DoD Instruction 7600.02, Audit Policies;
13) DoD Manual 7600.07, DoD Audit Manual.

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.

OMB control number not required; system does not collect records from 10 or more members of the public in a 12-month period.