

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:

Digital Media Examination Network (DMEN)

2. DOD COMPONENT NAME:

Department of Defense Inspector General

3. PIA APPROVAL DATE:

06/09/22

Defense Criminal Investigative Service (DCIS)

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.

DMEN provides an enterprise-wide repository for evidence collected during the course of a Defense Criminal Investigative Service (DCIS) investigation. DMEN serves the law enforcement community by allowing access to Defense Criminal Investigative Organizations (DCIOs) and other Federal law enforcement (FLE) and Intelligence Community (IC) agencies to review the evidence in their respective case(s). Other DoD OIG components, having a mission necessity and a need-to-know, may also be provided role-based access to DMEN. Additionally, the Department of Justice (DOJ) U.S. Attorney Offices (USAOs) may have access to DMEN to review evidence and make informed judgments on those individuals that may have committed a criminal act. Evidence is collected when search warrants and/or subpoenas are issued and enforced.

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)

Information is collected during the execution of a search warrant and/or subpoena. Information is used by DoD OIG, DCIOs, FLE and IC agencies, and USAOs to collaborate and coordinate investigative and disciplinary efforts.

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.

Information is used, collected, and maintained in accordance with 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 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 collected during the execution of a search warrant and/or subpoena; therefore, individual consent is not required.

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.)

- | | | |
|--|---|--|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory | <input checked="" type="checkbox"/> Not Applicable |
|--|---|--|

DMEN does not collect information directly from an individual.

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

- | | | |
|--|----------|--|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. | DCIS and other DoD OIG components |
| <input checked="" type="checkbox"/> Other DoD Components | Specify. | DCIOs |
| <input checked="" type="checkbox"/> Other Federal Agencies | Specify. | DOJ, IC agencies, and other FLE agencies |
| <input checked="" type="checkbox"/> State and Local Agencies | Specify. | State and local law enforcement agencies |
| <input type="checkbox"/> 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. | |
| <input type="checkbox"/> 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)

- | | |
|---|--|
| <input checked="" type="checkbox"/> Individuals | <input checked="" type="checkbox"/> Databases |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | <input checked="" type="checkbox"/> Commercial Systems |
| <input checked="" type="checkbox"/> Other Federal Information Systems | |

All sources could be used for collecting PII which will assist in the criminal investigation being conducted.

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

- | | |
|--|---|
| <input checked="" type="checkbox"/> E-mail | <input checked="" type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact | <input checked="" type="checkbox"/> Paper |
| <input checked="" type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input type="checkbox"/> Information Sharing - System to System | <input checked="" type="checkbox"/> Website/E-Form |
| <input checked="" type="checkbox"/> Other (If Other, enter the information in the box below) | |

PII can be collected from IT equipment and other electronic storage devices. Information is collected during the execution of a search warrant and/or subpoena.

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://dpcl.d.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 DMEN by using a personal identifier.

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.

Records are retained and disposed of in accordance with applicable disposition schedules. Any unscheduled records will be retained indefinitely, until they have been scheduled with the National Archives and Records Administration and have become eligible for disposition under those schedules

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.

The authority for collecting PII is granted through the following:

Public Law 95-452, Inspector General Act of 1978, as amended;

10 USC 1585a, Special agents of the Defense Criminal Investigative Service; authority to execute warrants and make arrests; and

DoD Directive 5106.1, Inspector General of the Department of Defense.

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.

DMEN is exempt from obtaining an OMB number as per DoD Manual 8910.01, Volume 2, Enclosure 3, paragraph 8a(2), which specifies an exemption for investigative information based on the following: "Exempt collections of information are those conducted (a) during the conduct of a federal criminal investigation or prosecution, or during the disposition of a particular criminal matter, and (b) during the conduct of a civil action to which the United States is a party, or during the conduct of any administrative action, investigation, or audit involving a government agency against specific individuals or entities."