

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:

DPAA Mission Applications (DMA) / Agency Information Management Systems (AIMS)

2. DOD COMPONENT NAME:

Defense POW/MIA Accounting Agency

3. PIA APPROVAL DATE:

08/25/2026

Under Secretary of War for Personnel and Readiness

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
- ☒ 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
- ☒ 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.

The DPAA Mission Applications system (also known as the Case Management System) is the secure, central computer system used by the Defense POW/MIA Accounting Agency to support our mission to find, identify, and account for missing U.S. military personnel and civilians from past conflicts. The system serves as a secure digital library and research database that helps our historians, field recovery teams, and laboratory scientists work together. It combines several secure tools: a digital document archive to store scanned historical papers, a laboratory database to manage scientific analysis, data reporting tools, and a workflow application to track case progress from initial research to final identification. To help us locate and identify missing Americans, the system stores historical military career files, wartime casualty reports, physical descriptions, dental records, and family DNA reference indicators. Other records included in the system are operational and information reports, biographic records, physical descriptions, personal statements and correspondence, returnee debriefings, interviews and media reports. It also securely stores contact information for living family members (next-of-kin) so to allow for communication directly with families and provide them with regular, official updates on their loved one's case, and allow for family member event registration and participation.

Information collected on missing U.S. military personnel and civilians includes: Name, date of birth, place of birth, country of citizenship, race, ethnicity, sex, religious preference, active duty information (place of entry, date of entry, home of record), branch of military service, rank/pay grade, biometric information (e.g. hair color, eye color, height, weight), casualty information (type, status, date of casualty, place of casualty circumstances, duty status) dental records, serial/service number or DoW Identification (DoW ID) number, and field search case number or source reference number (in the case of a classified source). While no longer collected or used to retrieve records, the social security number may be included in the records of individuals who went mission prior to the DoW ID Number replacing the SSN as the Geneva Convention serial number.

Information collected on next-of-kin includes: Full name, personal phone number, personal email address, home/mailling address, and family DNA reference samples.

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)

DPAA stores, collects and/or references PII data in historical records to support potential genealogy research requirements and/or data matching and mission-related use.

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.

The system maintains historical, wartime-era military personnel records and casualty files created by predecessor military organizations to

document losses as they occurred. Under 10 U.S.C. Chapter 76, the Agency is statutorily mandated to maintain a single, comprehensive case file for each unaccounted-for individual. Due to this statutory mandate and the historical nature of the archival records, individuals who are the subjects of these files do not have the opportunity to object to their maintenance. Family members, however, have the opportunity to object to data collected during official Family Member Update (FMU) events.

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.

No individuals do not have the opportunity to consent to the specific uses of their PII,. However, once collected the PII will only be used for those purposes stated above, as well as the SORN and any applicable Privacy Act Statement.

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: 10 U.S.C. 136, Under Secretary of Defense for Personnel, and Readiness; 10 U.S.C. Chapter 76, Missing Persons (sections 1501 through 1513); and DoD Directive 5110.10, Defense POW/MIA Accounting Agency (DPAA).

PURPOSE: To collect and maintain contact information to allow for communication directly with families and provide them with regular, official updates on their loved one's case, and allow for family member event registration and participation.

ROUTINE USES: Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended. Pursuant to 5 U.S.C. 552a(b)(3), records may be disclosed as a routine use to a domestic or foreign entity that has entered into a public-private partnership with the Defense POW/MIA Accounting Agency (DPAA) as authorized by 10 U.S.C. 1501a, when DPAA determines that such disclosure is necessary to the performance of services DPAA has agreed shall be performed by the partner. A complete list of routine uses may be found in the applicable System of Records Notice, DUSDP 11, POW/MIA Personnel Files at: <https://doc.defense.gov/DIRECTORATES/Privacy-and-Civil-Liberties-Directorate/Privacy/SORNsIndex/Article/4014369/dusdp-11/>

DISCLOSURE: Voluntary. However, failure to provide requested information may result in inability to participate in events or receive communication from DPAA.

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)

☒ Within the DoD Component	Specify.	Agency staff that communicate with the public
☒ Other DoD Components (i.e. Army, Navy, Air Force)	Specify.	Service Casualty Offices for each Military Service
☒ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)	Specify.	Federal Agencies that have entered into a public-private partnership with DPAA
☐ State and Local Agencies	Specify.	
☒ 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.	The contractor (Na Kupuna) performs the Mission Information Systems and Applications (MISA) services under HQ003423C0055
☒ Other (e.g., commercial providers, colleges).	Specify.	Domestic and foreign industry and academic partners with a partnership arrangement with DPAA

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 in DPAA system originates from existing DoD information systems, archival records, service casualty officers or directly through correspondence with members of the public. These systems include: Defense Casualty Information Processing System (DCIPS) & DPAA public website forms (powered by DPAA's Salesforce system).

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)

- ☒ In-Person Contact
 ☒ Paper
- ☐ Fax
 ☒ Telephone Interview
- ☒ Information Sharing - System to System
 ☒ 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
 ☐ 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.

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.

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

(3) Retention Instructions.

Permanent. Cut off (and convert to electronic format as necessary) once missing service members are accounted for, or upon case closure. Pre-accession to NARA 5 years after cutoff and transfer ownership to NARA 25 years after cutoff.

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.

10 U.S.C. 136, Under Secretary of Defense for Personnel, and Readiness; 10 U.S.C. Chapter 76, Missing Persons (sections 1501 through 1513); DoD Directive 5110.10, Defense POW/MIA Accounting Agency (DPAA); 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.

Minimal information