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:

Armed Forces Medical Examiner System (AFMES) Local Area Network MEDCOI

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

09/26/24

Armed Forces Medical Examiner System (AFMES)

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.

The Armed Forces Medical Examiner System (AFMES) Local Area Network Medical Community of Interest (MedCOI) is a Government developed system providing medical examiners the ability to track and record autopsy information, and to issue death certificate for decedents. The Armed Forces Medical Examiner System (AFMES) establishes a Department of Defense (DOD) standard system for medico-legal investigations. AFMES provides all workflow controls from intake through processing the release of remains, and it is used by different groups of users such as medical examiners, mortuary personnel and casualty officers. It provides medical examiners a tool for managing a decedent case from the time of notification of death, the determination of cause and manner of death, the identification of remains, the issuance of a death certificate, and to the final release of remains to a mortuary for preparation for interment. Teams provide a complete, multi-faceted forensic investigation. Provide worldwide scientific consultation, research and education services in the field of forensic DNA analysis to the Department of Defense and other agencies, provides DNA reference specimen collection, accession, and storage of United States military and other authorized personnel.

Personally Identifiable Information (PII) this system collects and manages includes demographic data, medical information, and military record related PII information. Categories of individuals include: deceased military members of all branches to include National Guard and Coast Guard; active duty and military reserve employees; federal contractors; foreign nationals employed by the federal government; deceased federal employees; federal contractors; foreign nationals employed by the federal government; and civilians whose deaths occur or are pronounced within Federal jurisdiction.

The system is owned by the Armed Forces Medical Examiner System (AFMES) and managed by AFMES IT department. It contains the Laboratory Information System Application (LISA) with Specimen Management System (SMS) module and Armed Forces Medical Examiner Tracking System (AFMETS) each having their own PIA using the AFMES eMASS ID.

The AFMES MedCOI includes system components, applications, electronic collections, and medical devices which have their own Privacy Impact Assessments in place. The AFMES IT department will ensure required DD 2930s unique to our location are submitted.

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 is collected for mission-related use to support decedent case information provided to Defense Casualty Information Processing System (DCIPS) and the Federal Bureau of Investigations (FBI).

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.

Individuals do not have the opportunity to object to the specific uses of their PII as the information is entered post-mortem. AFMETS is not the initial point of collection of the PII.

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.

Individuals do not have the opportunity to consent to the specific uses of their PII as the information is entered post-mortem. AFMETS is not the initial point of collection of the PII.

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

Although AFMETS collects PII primarily through information sharing between existing Department of Defense ("DoD") information systems, some PII is collected by AFMES in interviews of living individuals. Because AFMES collects PII directly from individuals, stored in a system of records and retrieved by a personal identifier, a Privacy Act Statement is provided for those instances of collection. The below Privacy Act Statement is provided to living individuals before they are asked to provide any of the information requested by AFMES.

AUTHORITY: 5 USC Section 301; 10 USC Section 3012; Public Law 91-121, Section 404 (A)(2); 10 USC Section 1471, Public Law 106-65; 10 USC Section 176 & 177: Public Law 94-361; DoD Directive 5154.24; DoD Instruction 5154.30; EO 9397 (SSN) as amended, and Deputy Secretary of Defense (Health Affairs) Memorandum, 16 December 1991, Subject: DOD DNA Registry.

PRINICIPAL PURPOSES: To establish a DNA Reference Specimen Repository and Database of information from kindred family members of unaccounted for/unidentified service members or other individuals needing to be identified. DNA is extracted from a biological specimen or personal effect, and be used in identifying human remains.

ROUTINE USE: None

DISCLOSURE: Voluntary. Failure to provide a reference sample or requested information may render DNA identification impossible.

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.	Defense Health Agency
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Medical examiners within the US Army Medical Command and casualty branches and military mortuaries.
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Federal Bureau of Investigations (FBI), Peace Corps, Department of State (DOS).
☐ 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.	Contract Company: Future Technology Incorporated (FTI) The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect all Government data; ensure the confidentiality, integrity, and availability of Government data in compliance with applicable laws and regulations, including data breach reporting and response requirements, per DFAR Subpart 224.1 (Protection of Individual Privacy), DoDD 5400.11, DoD Privacy Program, and DoD 5400.11-R, DoD Privacy Program. The contractor shall also comply with federal laws relating to freedom of information and records management. The Contractor shall comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191), as implemented by the HIPAA Privacy and Security Rules codified at 45 CFR. Parts 160 and 164, and as further implemented within the Military Health System (MHS) by DoDM 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoDI Health Care Programs and DoD 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs. The Contractor shall comply with applicable HIPAA related rules and regulations as they are published and as further defined by later-occurring Government requirements and DoD guidance, including current and forthcoming DoD guidance implementing applicable amendments under the American Recovery and Reinvestment Act of 2009 (ARRA). Any rules and regulations published, and/or requirements defined after the award date of this contract, and require expenditure of additional Contractor resources for compliance, may be considered "changes" and will be subject to the "changes" clause under the contract.
☐ 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

The PII collected is obtained from the Defense Casualty Information Processing System (DCIPS), records, and reports and other investigators.

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)*

The PII collected is manually entered into this system as well as auto-populated from DCIPS.
Official Form: AFMES Form 3: Request for Autopsy Report and Supplemental Information is available at: https://www.health.mil/Military-Health-Topics/Combat-Support/Armed-Forces-Medical-Examiner-System/Office-of-the-Armed-Forces-Medical-Examiner?type=Forms+%26+Templates#RefFeed

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://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.

The MTF MedCOI is not a system of records; however, system components, applications, and electronic collections within the enclave might require a SORN. Refer to the specific system component, application, or electronic collection PIA for SORN information.

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. Not Applicable

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

(3) Retention Instructions.

The LAN/Enclave itself does not have a NARA approved, pending, or GRS authority and retention instructions applied as a whole. Refer to NARA approved, pending, or GRS authority and retention instruction specific to the systems, applications, electronic collections, file servers, and share drives contained within the LAN/Enclave

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.

5 USC. 301, Departmental Regulations; 10 USC 131; 10 USC 3013, Secretary of Army; 10 USC 5013, Secretary of the Navy; 10 USC 8013, Secretary of the Air Force; EO 9397 (SSN); Deputy Secretary of Defense memorandum dated December 16, 1991; and Assistant Secretary of Defense (Health Affairs) memoranda dated January 5, 1993, March 9, 1994, April 2, 1996, and October 11, 1996.

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.

The MTF MedCOI does not collect information from members of the public; however, system components, applications, or electronic collections within the MTF MedCOI may. Refer to the specific sub-system, application, or electronic collection PIA for information regarding the OMB Control Number.