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:

Laboratory Information System Application (LISA) with Specimen Management System (SMS) module

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

09/23/24

AFMES Program Management Office (PMO)

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 Laboratory Information System Application (LISA) is used by Forensic deoxyribonucleic acid (DNA) Scientists at the Armed Forces Medical Examiner System (AFMES) to manage the entire DNA laboratory process, from receipt of evidence to reporting out the identification of deceased service members, the research of new technologies to aid in identifications, the receipt and maintenance of the family reference database and database samples, the quality control of all instruments and reagents used in human DNA identification testing, and inventory controls for ordering of supplies used in the laboratories and offices. LISA has a Public Key Infrastructure (PKI) enabled .mil-only accessible web interface hosted by U.S. Army Medical Research and Development Command (USAMRDC) within a demilitarized zone (DMZ) and is used exclusively by Regional Medical Examiners in the performance of their official duties while deployed.

The LISA Specimen Management System (SMS) module is a database created by AFMES and used by the AFMES - Armed Forces Repository of Specimen Samples for the Identification of Remains (AFMES-AFRSSIR) to manage the collection, storage and retrieval of bloodstain reference cards for DNA identification of human remains. The SMS module interfaces between the Defense Enrollment Eligibility Reporting System (DEERS) database. DMDC provides a web service interface for the SMS client to send SOAP/XML requests over HTTPS. The specimen processors enter the last name and Social Security Number (SSN) or Electronic Data Interchange Personnel Identifier (EDIPI) off of the donor card into the SMS client, which sends a request to DEERS to look up the official DEERS demographic information for the specimen card donor. DEERS demographic information returned is then used to populate the SMS record for the specimen card. Once the card entry is complete, a return flag is sent to DEERS for the donor indicating there is an acceptable specimen card on file.

The types of Personally Identifiable Information (PII) that LISA collects include the following: demographic information, personal contact information, Social Security Numbers (SSN), other identification numbers, biometrics, military records, family information, adoption information, and system user information.

The categories of individuals on whom PII is collected include the following: World War II, Korean War, Vietnam War, and the Cold War; Active Duty; Reserve; National Guard; Coast Guard and Coast Guard Reserve; civilian federal employees; foreign national employees; contract employees; individuals who hold the roles of service members and/or persons identified of interest to the Department of Defense (DoD), and who require positive identification on behalf of local and state partners or other law enforcement or investigative entities; and dependents and/or other relations, where appropriate, in order to establish kinship; AFMES staff members for the establishment of DNA elimination databases; and family members of missing service members needed to establish kinship.

The LISA with SMS Module is owned and managed by the AFMES Program Management Office (PMO).

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)*

PII is collected for mission-related purposes to ensure the readiness of active duty military and for the rapid identification of current day casualties; the rapid identification of missing service members from World War II, Korean War, Vietnam War and the Cold War; and to assist with establishing kinship. The intended use of the PII is for identification and verification purposes to match individuals with the DNA family reference sequence data stored in the LISA system and with DNA reference card information stored in the LISA-SMS module.

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.

LISA: The collection of family member PII on DNA Form 332 Informed Consent Form – v9.0W RELEASED ON: 6/22/2016 and the donation of a DNA reference specimen is voluntary. Individual family members simply decline the collection by not electing to fill out DNA Form 332 Informed Consent Form and do not provide a DNA reference sample.

LISA SMS Module: Individuals may object to the collection of their PII at the initial point of the requested collection, by indicating so in the bloodstain reference card. If DoD military personnel object, possible consequences include adverse administration action up to and including separation from federal service. If non-DoD personnel selected for the program object, possible consequences include exclusion from areas under the control of the U.S. Armed Forces and the hindrance of remains identification efforts.

Regarding PII collected through an interface with other systems - SMS, DEERS and DCIPS - individuals do not have the opportunity to object as LISA is not the initial point of collection. However, individuals may object to the collection of their PII per the methods described by those systems.

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.

LISA: DNA Form 332 Informed Consent Form – v9.0W RELEASED ON: 6/22/2016 requests consent for additional use of collected samples. Individuals have the right to refuse their samples to be used for additional testing outside of establishing kinship. Refusal of consent for additional testing, will in no way affect the use of sample(s) for identification of their missing service member. The PII for this application is not always collected directly from the individual.

LISA SMS module: For the mandatory DNA bloodstain cards, individuals are required to sign the bloodstain reference card upon completion. The card includes a Privacy Act Statement which explains how the PII will be used. Providing the PII requested on the bloodstain card is mandatory for DoD military personnel, and possible consequences for failing to respond include adverse administrative action up to and including separation from federal service. If non-DoD personnel selected for the program object, possible consequences include exclusion from areas under the control of the U.S. Armed Forces and the hindrance of remains identification efforts.

Regarding PII collected through an interface with other systems - SMS, DEERS and DCIPS - individuals do not have the opportunity to consent as LISA is not the initial point of collection. However, individuals may give or withhold consent to specific uses of their PII per the methods described by those systems.

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

LISA DNA Form 332
In accordance with the Privacy Act of 1974 (Public Law 93-579), this notice informs you of the purpose of the form and how it will be used. Please read it carefully.
AUTHORITY: 10 U.S.C. §1471; Public Law 104-191; Deputy Secretary of Defense Memorandum, "Establishment of a Repository of Specimen Samples, December 16, 1991; and DoDI 5154.30.
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 will be extracted from a biological specimen or personal effect and used in identifying human remains.
ROUTINE USE: Use and disclosure of your records outside of DoD may also occur in accordance with the DoD Blanket Routine Uses published at http://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.html and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a(b)). Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD.

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)*

[X] Within the DoD Component	Specify.	Defense Health Agency Health Care Administration AFMES
[X] Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	SMS module: Army, Navy, Marine, and Air Force medical readiness programs
[X] Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	National Transportation Safety Board (NTSB)
[ ] State and Local Agencies	Specify.	
[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.	Contracting Company: Future Technology Incorporated (FTI) Contracting Language: The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect Government data. The Contractor shall ensure the confidentiality, integrity, and availability of Government data per applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 which incorporates by reference DoDD 5400.11, and DoD 5400.11-R, The contractor shall comply with federal laws relating to freedom of information and records management. The Contractor shall comply with requirements of 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 C.F.R. Parts 160 and 164, and as further implemented within the Military Health System (MHS) by DoD 6025.18-R, and DoD 8580.02-R, 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).
[ ] 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] Existing DoD Information Systems
- [X] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

Existing DoD Information Systems: Defense Civilian Intelligence Personnel System (DCIPS); Defense Enrollment Eligibility Reporting System (DEERS)

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

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

PII may be collected from individuals in-person, via postal mail, and Online using: Bloodstain DNA Reference Card; Family Reference Donor Card; Family Reference Buccal Swa; Family Reference Collection Form DNA Form 332 – v9.0W

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 A0040-57a DASG

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. Unscheduled

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

(3) Retention Instructions.

Unscheduled - Permanent. Treat system and/or records maintained in the system as permanent until a NARA approved schedule and disposition authority has been applied.

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, Office of the Secretary of Defense; 10 USC 3013, Secretary of Army; 10 USC 5013, Secretary of the Navy; 10 USC 8013, Secretary of the Air Force; Deputy Secretary of Defense Memorandum 16 December 1991; and Assistant Secretary of Defense (Health Affairs) Memorandum 5 January 1993, 9 March 1994, 2 April 1996, and 11 October 1996; SMS Module: DoD Manual 8910.01, Volume 2, DoD Information Collections Manual: Procedures for DoD Public Information Collections 2.b. (1); states: "This volume does not apply to Component internal information collections that do not collect information from members of the public memorandum 5 January 1993, 9 March 1994, 2 April 1996, and 11 October 1996; EO 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 [X] 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.