PRIVACY IMPACT ASSESSMENT (PIA)

For the

AUTOMATED FINGERPRINT SYSTEM - LAPTOP L-1 Identity Solutions CAFIS, Fusion and all other L-1 Biometric Systems (AFS-LAPTOP)
DEPARTMENT OF THE ARMY

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 12581/DA197495
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier A0380-67 DAMI

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
10 U.S.C. 3013; 50 U.S.C. 4039; and the National Security Act of 1947; E.O. 10450 and 10865; and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Biometrics is an important enabler that shall be fully integrated into the conduct of DoD activities to support the full range of military operations. Biometric collection, transmission, storage, caching, tagging, and use shall be controlled through the use of DoD-approved national, international, and other consensus-based standards, protocols, best practices, and equipment to ensure consistency and support interoperability.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

GAO-08-536 "Alternatives Exist for Enhancing Protection of Personally Identifiable Information,"May 2008
Methodology:
GAO analyzed privacy laws and guidance (Privacy Act, E-Gov Act, Paperwork Reduction Act and OMB guidance), compared them with the Fair Information Practices, and obtained perspectives from federal agencies and an expert forum.
•They may not consistently protect personally identifiable information (PII) in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles.
•Based on discussions with privacy experts, agency officials, and analysis of laws and related guidance, the GAO identified three major areas.
1. Applying privacy protections consistently to all federal collection and use of personal information.
•The Privacy Act's definition of a "system of records"(any grouping of records containing personal information retrieved by individual identifier), which sets the scope of the Act's protections, does not always apply whenever personal information is obtained and processed by federal agencies.
•If agencies do not retrieve personal information by identifier, the Act's protections do not apply.
2. Ensuring that collection and use of personally identifiable information is limited to a stated purpose.•According to the purpose specification, collection limitation, and use limitation principles, the collection of personal information should be limited, and its use should be limited to a specified purpose.
•Current laws and guidance impose only modest requirements for describing the purposes for collecting and using personal information and limiting how that information is collected and used.
•Agencies are not required to be specific in formulating purpose descriptions in their public notices.
3. Establishing effective mechanisms for informing the public about privacy protections.
•According to the openness principle, the public should be informed about privacy polices and practices, and the accountability principle calls for those who control the collection or use of personal information to be held accountable for taking steps to ensure privacy protection.
•Public notices are a primary means of establishing accountability for privacy protections and giving individuals a measure of control over the use of their personal information.
•Yet concerns have been raised that Privacy Act notices may not serve this function well.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. DOD Biometric Information Management Agency (BIMA)

☒ **Other DoD Components.**

Specify. SOCOM, JSOC

☒ **Other Federal Agencies.**

Specify. Department Of Homeland Security (DHS), Federal Bureau of Investigations (FBI), Office of Personnel Management (OPM)

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

By objecting, this person's security clearance will not be processed.
Homeland Security Presidential Directive- 6 "Integration and Use of Screening Information"
Homeland Security Presidential Directive- 11 "Comprehensive Terrorist-Related Screening Procedures"
Homeland Security Presidential Directive- 12 "Policy for a Common Identification Standard for Federal Employees and Contractors"
Federal Information Processing Standard (FIPS) 201
Executive Order 13356 "Strengthening the Sharing of Terrorism Information to Protect America"
OMB M-04-04 "E-Authentication Guidance for Federal Agencies"
DSD memorandum, 27 December 2000, "Executive Agent for the Department of Defense (DOD) Biometrics Project"

(2) If "No," state the reason why individuals cannot object.

j. 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.

By objecting, this person's security clearance will not be processed.
Homeland Security Presidential Directive- 6 "Integration and Use of Screening Information"
Homeland Security Presidential Directive- 11 "Comprehensive Terrorist-Related Screening Procedures"
Homeland Security Presidential Directive- 12 "Policy for a Common Identification Standard for Federal Employees and Contractors"
Federal Information Processing Standard (FIPS) 201
Executive Order 13356 "Strengthening the Sharing of Terrorism Information to Protect America"
OMB M-04-04 "E-Authentication Guidance for Federal Agencies"
DSD memorandum, 27 December 2000, "Executive Agent for the Department of Defense (DOD) Biometrics Project"

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- ☒ **Privacy Act Statement**
- ☐ **Privacy Advisory**
- ☐ **Other**
- ☐ **None**

Describe each applicable format.

Privacy Act Statement:

Your privacy is important to us, and maintaining your trust and confidence is one of our highest priorities. We respect your right to keep your personal information confidential and understand your desire to avoid unwanted solicitations.

Types of information we collect: interviews and phone calls with you, letters or e-mails from you and fingerprint card information.

Confidentiality and Security of Non-public Personal Information: Except as otherwise described in this notice, we restrict access to non-public personal information about you to employees who must use that information to provide services to you. We also maintain physical, electronic, and procedural safeguards in compliance with applicable laws and regulations to guard your personal information from unauthorized access, alteration, or premature destruction. Please call us if you have any questions or if we can be of further service.