PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Fingerprint Suite (eFP)
Defense Commissary Agency

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	
☐	**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

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	SF-87 Control Number: 3206-0150 FD-258 Control Number: 1110-0046
Enter Expiration Date	3206-0150: 3/31/16; 1110-0046: 5/31/13

☐ **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.

1. Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, December 17, 2004, Security and Suitability Process Reform, February 2010

2. Executive Order 13467, Homeland Security Presidental Directive 12

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.

To electronically capture and transmit fingerprints in support of background investigations (for newly hired employees and or clearances).

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

PII contained within eFP will include, but is not limited to, an individual's: address, date of birth, and social security number. A breech of this information could allow an individual's identity to be stolen. Mitigations to these risks include: fingerprint records (hard and soft copy) are accessed by limited person(s) responsible for servicing the record system in performance of their official duties, and by authorized personnel who are properly screened and cleared for need-to-know. It is up to the administrators to ensure this requirement is complied with before access is granted. Electronic fingerprint records that contain PII are stored in computer storage devices protected by computer system software. Once successfully transmitted to OPM, the software can be configured to be automatically delete individual electronic fingerprint records from the laptop that hosts the Electronic Fingerprint Suite. The host laptop is also located in a secured room which is controlled by a key lock. This room is only accessible to those individuals employed by the DeCA Security Office/DeCA Inspector General's Office that have a need to use the system. The first measure of physical access inside the DeCA consists of pass card entry, which is granted to DeCA employees. The second measure of physical access to the room containing the laptop with the eFP software is by a controlled key and lock.

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. Human Resources, Security Office

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. OPM, FBI

☐ **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.

Per SF 85; SF 85p; and SF 86; Providing PII is voluntary. The individual may choose not to provide each item of requested information. However, the investigating agency will not be able to complete the individual's investigation, which will adversely affect that individual's eligibility for a national security position or non-sensitive positions. All employees, applicants, and contractors submit investigations voluntarily. This information is reflected in the instructions for the afore-mentioned forms.

(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.

Yes, applicants, appointees, and contractors submit a minimum of two signed releases of information forms (i.e. SF 85, SF 86) during the investigative process for a new hire and or security clearance suitability. The fingerprints are a basic element of any background investigation. Individuals may refuse to participate at any time during the investigative process.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.	Both of the hard copy fingerprint cards, SF-87 and FD-258, have Privacy Statements incorporated in the "how to complete" instructions and the applicant is referred to the Privacy Act Statement when submitting hardcopy (ink rolled) or soft copy (electronic) fingerprints.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.