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:

Secure Web Fingerprint Transmission (SWFT)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

05/16/25

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.

Secure Web Fingerprint Transmission (SWFT) is a secure web-based Department of Defense (DoD) enterprise system that allows submission of standard electronic fingerprints (e-fingerprints) to DCSA for persons who require an investigation for government employment, security clearances, or entry into the armed forces. SWFT eliminates paper-based capture and handling of fingerprints, expedites the background check process by reducing invalid fingerprint submissions, and provides end-to-end accountability for sensitive PII.

Authorized users, such as DoD agencies or cleared DoD contractors, collect and securely transmit e-fingerprints to SWFT for subsequent transmittal to DCSA. The SWFT system uses PII data for distinct identification of each electronic fingerprint file and the information is passed to the Fingerprint Transaction System (FTS) for matching with the applicant's fingerprint image. E-fingerprints received are then transmitted to the Federal Bureau of Investigation (FBI) for processing as part of the investigation.

Types of personal information collected in SWFT include: Social Security Number, Full Name, Date of Birth, Place of Birth and Biometric information.

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 and used for data matching within SWFT- and other applications to which SWFT submits the electronic fingerprint file.

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 does not directly present individuals the opportunity to object. Individuals voluntarily complete the SF85, SF85P, SF86, SF87 or FD-258 for purposes of conducting background investigations. At that time of collection, they have the opportunity to object.

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.

The system does not directly present individuals the opportunity to object. Individuals voluntarily complete the SF85, SF85P, SF86, SF87 or FD-258 for purposes of conducting background investigations. At that time of collection, they have the opportunity to object.

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

Under the Privacy Act of 1974, you must safeguard personal information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section552a Public Law 93-579, DoDD5400.11, DoDR 5400.11-R and the applicable service directives.

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.	DCSA/PEO/PSS
☐	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
☐	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.	
☐	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

Fingerprinting Official collects information directly from individual and upload into SWFT. SWFT receives eFTP files via Secure File Gateway (SFG) from external agencies.

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)*

PII is manually typed into a scanner software application and then married to the fingerprint images to create a .EFT file. That .EFT file is then uploaded or relayed into SWFT through direct upload, the SWFT+ application or an SFG relay transfer.

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 DUSDI 02-DoD Personnel Vetting Recor

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. DAA-0446-2024-0003

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

(3) Retention Instructions.

Destroy all electronic fingerprints and demographic information 120 days after SWFT receipt.

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.

EO 13467, as amended; DoD Directive 5105.42, DCSA; DoD Instruction 5200.02, DoD Personnel Security Program (PSP); 32 CFR part 156, DoD Personnel Security Program; EO 10450 Security Requirements for Government employment; HSPD 12, Policy for a Common identification standard for Federal employees and Contractors; and 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 ☒ 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.

It has been concluded that because SWFT is only a store-and-forward system for electronic fingerprints, and does not serve as a permanent repository of the data that it receives, serving only as a time-limited temporary distribution point for electronic fingerprints, that an OMB number is not required. It is exempt from having its own OMB control number due to the information collected is already covered by another active OMB Control Number. SF-87: Fingerprint Chart, 0705-0002, April 2027
FD-258: Standard Fingerprint Form (FBI), 1110-0046 (FBI Managed)