

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:

National Background Investigation Services - Secure Web Fingerprint Transmission (NBIS-SWFT)

2. DOD COMPONENT NAME:

If Other, enter the Component name in the box below.

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

05/25/22

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- ☐ From members of the general public ☒ From Federal employees and/or Federal contractors
- ☐ From both members of the general public and Federal employees and/or Federal contractors ☐ 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, and Place of Birth.

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 cleared individuals on whom the PII will be collected have given permission for information to be collected by voluntarily filling out the SF 85 and/or SF 86 Questionnaire for National Security Positions. Both the SF85 and SF86 state "The information you provide on this form,

and information collected during an investigation, may be disclosed without your consent by an agency maintaining the information in a system of records as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses, a list of which are published by the agency in the Federal Register." Both the SF85 and SF86 list as a Routine Use, disclosure "to Executive Branch Agency insider threat, counterintelligence, and counterterrorism officials to fulfill their responsibilities under applicable Federal law and policy, including but not limited to E.O. 12333, 13587 and the National Insider Threat Policy and Minimum Standards given consent for data to be collected by voluntarily submitting the SF 85 or SF 86.

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.

PII in the system is voluntarily provided by individuals in connection with completion of Standard Forms 85 or 86, which include notices regarding consent for the investigation and routine uses of the information provided by the person being investigated.

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

The data in SWFT is collected via Standard Forms 85 and 86, which include Privacy Act advisements, and via form FD-258, Fingerprint Card, which provides the following Privacy Act Statement.

"Privacy Act Statement

This privacy act statement is located on the back of the FD-258 fingerprint card.

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

As of 03/30/2018

Additional Information:

NONCRIMINAL JUSTICE APPLICANT'S PRIVACY RIGHTS

As an applicant who is the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose (such as an application for employment or a license, an immigration or naturalization matter, security clearance, or adoption), you have certain rights which are discussed below. All notices must be provided to you in writing. 1 These obligations are pursuant to the Privacy Act of 1974, Title 5, United States Code (U.S.C.) Section 552a, and Title 28 Code of Federal Regulations (CFR), 50.12, among other authorities.

- You must be provided an adequate written FBI Privacy Act Statement (dated 2013 or later) when you submit your fingerprints and associated personal information. This Privacy Act Statement must explain the authority for collecting your fingerprints and associated information and whether your fingerprints and associated information will be searched, shared, or retained. 2
- You must be advised in writing of the procedures for obtaining a change, correction, or update of your FBI criminal history record as set forth at 28 CFR 16.34.
- You must be provided the opportunity to complete or challenge the accuracy of the information in your FBI criminal history record (if you have such a record).
- If you have a criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before the officials deny you the employment, license, or other benefit based on information in the FBI criminal history record.
- If agency policy permits, the officials may provide you with a copy of your FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, you may obtain a copy of the record by submitting fingerprints and a

fee to the FBI. Information regarding this process may be obtained at <https://www.fbi.gov/services/cjis/identity-history-summary-checks> and <https://www.edo.cjis.gov>.

• If you decide to challenge the accuracy or completeness of your FBI criminal history record, you should send your challenge to the agency that contributed the questioned information to the FBI. Alternatively, you may send your challenge directly to the FBI by submitting a request via <https://www.edo.cjis.gov>. The FBI will then forward your challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry. Upon receipt of an official communication from that agency, the FBI will make any necessary changes/corrections to your record in accordance with the information supplied by that agency. (See 28 CFR 16.30 through 16.34.)

• You have the right to expect that officials receiving the results of the criminal history record check will use it only for authorized purposes and will not retain or disseminate it in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council.³

1 Written notification includes electronic notification, but excludes oral notification.

2 <https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement>

3 See 5 U.S.C. 552a(b); 28 U.S.C. 534(b); 34 U.S.C. § 40316 (formerly cited as 42 U.S.C. § 14616), Article IV(c);

28 CFR 20.21(c), 20.33(d) and 906.2(d)."

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

☒ Within the DoD Component

Specify.

☐ Other DoD Components

Specify.

☒ Other Federal Agencies

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

The DCSA Defense Information System for Security (DISS) provides an outbound to SWFT report which lists all eQIP requests which have matching electronic fingerprint submissions that were received the prior day. The PII data provided on the report is for matching purposes and includes Social Security Number, Full Name, Date of Birth, and Place of Birth.

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)

☐ Face-to-Face Contact

☐ Paper

☐ Fax

☐ Telephone Interview

☐ Information Sharing - System to System

☒ Website/E-Form

☐ Other (If Other, enter the information in the box below)

Applicants provide information in support of their personal background investigation. The biometric and biographic information is collected in two ways and transmitted to SWFT; 1) biographic and biometric information is integrated into e-Fingerprint files on local fingerprinting workstations, 2) biographic and biometric information is integrated into e-Fingerprint files in the SWFT system. These e-Fingerprint files, including the PII, are transmitted to and stored in SWFT.

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://dpcl.d.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.

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

(3) Retention Instructions.

Destroy closed cases involving potentially actionable issues 25 years after the end of eligibility. Destroy all other closed cases 16 years after the end of eligibility.

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 statute 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.