NBIS-SWFT ACCESS, REGISTRATION, AND TESTING PROCEDURES

VERSION 3.10

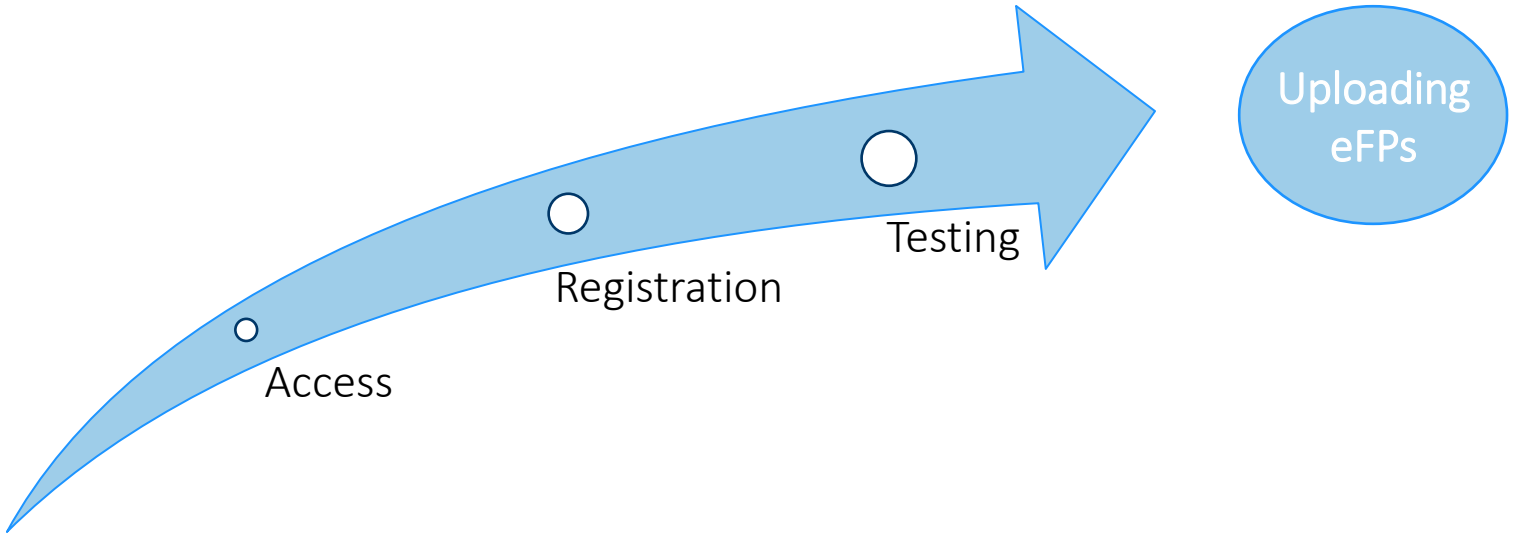
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Dated August 2022

Please refer to the NBIS-SWFT Access, Registration, and Testing Procedures document for more detailed information.

Getting Started

An Authorized Organization Representative must complete three phases before a cleared National Industrial Security Program (NISP) organization, U.S. Military component, or Department of Defense (DoD) agency can submit electronic fingerprints (eFPs) to the National Background Investigation Services-Secure Web Fingerprint Transmissions (NBIS-SWFT) Web Application. NBIS-SWFT and SWFT can be used interchangeably, with SWFT being used within this power point.



Getting Started

Access

Access to SWFT can be granted to the following users:

- NISP cleared organizations
- U.S. Military components and DoD agencies

SWFT users require a Public Key Infrastructure (PKI) certificate stored on a medium security hardware token to access SWFT.

All users are required to obtain a DoD approved Smart Card:

- Common Access Card (CAC)
- External Certificate Authority (ECA)
- Personal Identity Verification (PIV)
- Personal Identity Verification-Interoperable (PIV-I) credential

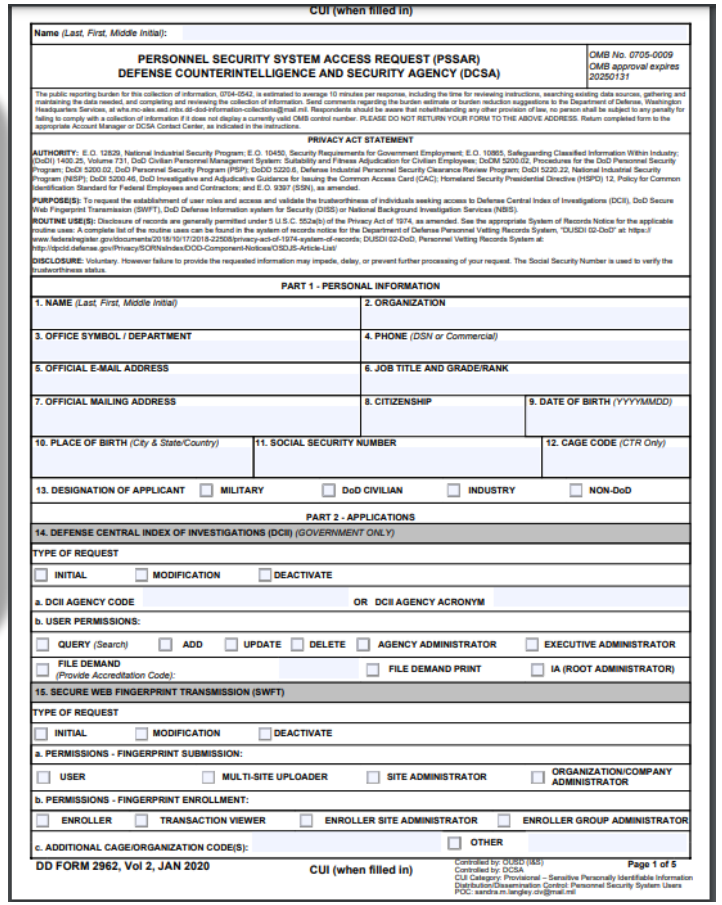
Access (Personnel Security System Access Request (PSSAR))

Each organization with a fingerprint processing facility must appoint an Organization Administrator or Site Administrator. To obtain a SWFT account, all applicants must complete and submit a Personnel Security System Access Request (PSSAR).

Completed PSSAR forms for Organization Administrators must be submitted to the Defense Counterintelligence and Security Agency (DCSA) Customer Engagements Team (CET).

PSSARs are available on the SWFT DCSA Website at ***https://www.dcsa.mil/is/swft/***. For SWFT users, this file is accessed by selecting *SWFT Resources> Access Request> PSSAR Form.* For WebEnroll users, this file is accessed by selecting *SWFT Resources> eFP Enrollment (SWFT+)> Access Request Form*. Go to slides 12 and 13 for details.

After obtaining a SWFT account, Organization Administrators or Site Administrators are responsible for processing PSSARs and creating and managing all other user accounts for their organization or facility. See the *NBIS-SWFT Administrator Guide* for details.



CUI (when filled in)

Name (Last, First, Middle Initial):

PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR)
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)

OMB No. 0705-0009
OMB approval expires 20250131

The public reporting burden for this collection of information, 0704-0542, is estimated to average 10 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. Return completed form to the appropriate Account Manager or DCSA Contact Center, as indicated in the instructions.

PRIVACY ACT STATEMENT

AUTHORITY: E.O. 12829, National Industrial Security Program; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoDM 5200.02, Procedures for the DoD Personnel Security Program; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, National Industrial Security Program (NISP); DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

PURPOSE(S): To request the establishment of user roles and access and validate the trustworthiness of individuals seeking access to Defense Central Index of Investigations (DCII), DoD Secure Web Fingerprint Transmission (SWFT), DoD Defense Information system for Security (DISS) or National Background Investigation Services (NBIS).

ROUTINE USE(S): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended. See the appropriate System of Records Notice for the applicable routine uses: A complete list of the routine uses can be found in the system of records notice for the Department of Defense Personnel Vetting Records System, "DUSDI 02-DoD" at https://www.federalregister.gov/documents/2018/10/17/2018-22508/privacy-act-of-1974-system-of-records; DUSDI 02-DoD, Personnel Vetting Records System at: http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/

DISCLOSURE: Voluntary. However failure to provide the requested information may impede, delay, or prevent further processing of your request. The Social Security Number is used to verify the trustworthiness status.

PART 1 - PERSONAL INFORMATION

1. NAME (Last, First, Middle Initial)	2. ORGANIZATION	
3. OFFICE SYMBOL / DEPARTMENT	4. PHONE (DSN or Commercial)	
5. OFFICIAL E-MAIL ADDRESS	6. JOB TITLE AND GRADE/RANK	
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP	9. DATE OF BIRTH (YYYYMMDD)
10. PLACE OF BIRTH (City & State/Country)	11. SOCIAL SECURITY NUMBER	12. CAGE CODE (CTR Only)

13. DESIGNATION OF APPLICANT ☐ MILITARY ☐ DoD CIVILIAN ☐ INDUSTRY ☐ NON-DoD

PART 2 - APPLICATIONS

14. DEFENSE CENTRAL INDEX OF INVESTIGATIONS (DCII) (GOVERNMENT ONLY)

TYPE OF REQUEST

☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE

a. DCII AGENCY CODE OR DCII AGENCY ACRONYM

b. USER PERMISSIONS:

☐ QUERY (Search) ☐ ADD ☐ UPDATE ☐ DELETE ☐ AGENCY ADMINISTRATOR ☐ EXECUTIVE ADMINISTRATOR

☐ FILE DEMAND (Provide Accreditation Code): ☐ FILE DEMAND PRINT ☐ IA (ROOT ADMINISTRATOR)

15. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)

TYPE OF REQUEST

☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE

a. PERMISSIONS - FINGERPRINT SUBMISSION:

☐ USER ☐ MULTI-SITE UPLOADER ☐ SITE ADMINISTRATOR ☐ ORGANIZATION/COMPANY ADMINISTRATOR

b. PERMISSIONS - FINGERPRINT ENROLLMENT:

☐ ENROLLER ☐ TRANSACTION VIEWER ☐ ENROLLER SITE ADMINISTRATOR ☐ ENROLLER GROUP ADMINISTRATOR

c. ADDITIONAL CAGE/ORGANIZATION CODE(S): ☐ OTHER

DD FORM 2962, Vol 2, JAN 2020 CUI (when filled in) Page 1 of 5

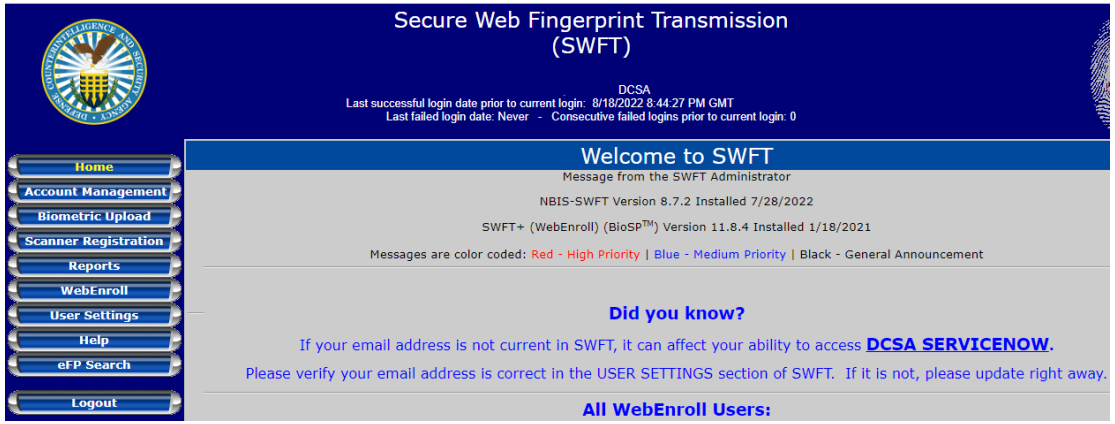
Controlled by: OUSD (I&S)
Controlled by: DCSA
CUI Category: Provisional – Sensitive Personally Identifiable Information
Distribution/Dissemination Control: Personnel Security System Users
POC: sandra.m.langley.civ@mail.mil

Getting Started

Registration

All fingerprint capture hardware and software must meet Federal Bureau of Investigation (FBI) certification guidelines. Each fingerprint enrollment workstation must be registered and tested with SWFT and must be approved by the Registration Authority.

An online Scanner Registration form is available in the SWFT Web Application, which provides an automated tool for registering a new fingerprint enrollment workstation or editing an existing registration. SWFT shares the registration data with the registration authority.



Getting Started

Testing

Every fingerprint capture system (live scan, card scan, or server platform) must be registered, tested, and approved for production by the registration authority before enrolling official biometric data.

The SWFT Coordinator monitors and administers the registration process for all fingerprint capture devices and coordinates scheduling and test activities for approval of devices. SWFT Coordinators also assist with resolution of potential issues with the test eFPs.

Re-registration and Re-testing

All fingerprint scanner equipment and software must be re-registered and re-tested under the following circumstances (contact the SWFT Coordinator when unsure):

- Any component of the fingerprint enrollment workstation is replaced (laptop, scanning device, or both)
- Hardware part repair or replacement
- Software replacement, upgrade, modification, or configuration change
- Transfer of the equipment to another location

SWFT Server/Platform Services

Scanner/Server Platform fingerprint systems typically involve two components: 1) One or more fingerprint scanning devices; 2) Server Platform that integrates fingerprint images and biographic data and generates the eFP file.

Multiple scanning devices can be connected to a single server. At least one scanner-server platform pair must be registered and tested with SWFT and the registration authority. The registration must prove that the hardware and software components in the server platform meet the FBI certification guidelines. The test of the scanner-server platform pair must prove that the system is properly configured and generates eFP files that comply with the FBI Electronic Biometric Transmission Specification (EBTS) and DCSA Fingerprint Transaction System (FTS) or other registration authority specifications.

Additional scanning devices that communicate with a server platform that have already been approved for production by SWFT and the registration authority must also be registered, but do not have to be tested. Scanning devices that connect to an approved server platform-must include in the comments section of the SWFT registration form a reference to the previously registered and approved server platform.

Submission of eFPs on Behalf of Other Organizations

Submission of eFPs

Option One: Multi-Site Uploader - Service Provider with Limited Privileges Submits Fingerprints on Behalf of Another Organization

Any SWFT account holder can act as a service provider for other Organizations if the "Multi-Site Uploader" permission is enabled for that account. This allows the service provider to submit eFPs for another Organization and generate reports that identify eFPs they uploaded on behalf of other organizations. Serviced Organizations must obtain their own SWFT Organization account before seeking services from a Service Provider.

Organizations are strongly encouraged to enter into a service agreement that will address handling and protection of the Personally Identifiable Information (PII) data. The "Multi-Site Uploader" permission requires submission of a valid PSSAR to the DCSA CET.

Note: Users with Multi-Site Uploader permission can upload eFPs for any Organization/Commercial and Government Entity (CAGE) Code that has been registered in SWFT. Once permission is granted, the Multi-Site Uploader does not need to seek SWFT pre-approval for uploading eFPs associated with any registered Org/CAGE Code. Organizations are encouraged to use their own SWFT accounts to monitor fingerprint transactions that have occurred on their behalf.

Submission of eFPs on Behalf of Other Organizations

Submission of eFPs

Option Two: Multi-Site SWFT Account - Service Provider Acts with Full Privileges to Submit Fingerprints on Behalf of Another Organization

A service provider must have their own SWFT account established under the organization for which it provides services. This account must be associated with one or more of the serviced organization's Org/CAGE Codes.

A SWFT account under the serviced organization grants the service provider the ability to submit eFPs on their behalf. The service provider can access SWFT reports and PII data for eFPs they submitted on behalf of their serviced organizations.

Each request for adding an additional Org/CAGE Code to an existing SWFT account requires a PSSAR approved by the appropriate nominating official from the serviced organization.

Note: It is not necessary to own and operate a fingerprint capture device to obtain a SWFT account or to submit eFPs. Organizations can submit eFP files that were generated by a Service Provider with a SWFT approved and registered workstation.

Submission of eFPs on Behalf of Other Organizations

Submission of eFPs

Option Three: A 3rd Party Service Provider is authorized to enroll (i.e., take) fingerprints and produce electronic fingerprint files, or submit e-fingerprints to SWFT, or both

3rd Party Service Providers must have their own hardware/software equipment, that has been registered, tested, and approved for SWFT production under their organization.

3rd Party Service Providers must be vetted to offer fingerprint services to DoD clients. Organizations intending to offer their fingerprint services to the DoD community should contact the SWFT Coordinator for qualification criteria and to initiate the vetting process.

The *Fingerprint Service Providers* list, published on the *SWFT DCSA* website at ***https://www.dcsa.mil/is/swft/***, lists DCSA vetted 3rd party service providers. Some service providers have offices in multiple geographical areas.

Access

Security officers and specialists who intend to use the services of a 3rd Party Service Provider for capturing the fingerprints and generating eFP files need to follow only Steps 1 through 3 in the Access portion of the ART Procedures. The Registration and Testing procedures are applicable only to applicants who intend to operate fingerprint enrollment workstations.

Your Organization must verify that the Organization/3rd Party Service Provider that will generate the eFPs for you had their equipment registered and approved for production by SWFT and the registration authority. Access to the verification tool requires a SWFT account.

To confirm the registration status of a fingerprint capture workstation, perform the following steps:

- Obtain either the scanning device Make and Serial Number, or the Org/CAGE Code from the Service Provider.
- Log in to SWFT.
- Access the Reports section and run the report “Scanner Registration Status by Hardware Vendor and Serial Number” or “Scanner Registration Status by Org/CAGE Code” as appropriate.

Access

Step 1: The Authorized Organization Representative obtains the appropriate PSSAR from the SWFT DCSA website at the following link: ***https://www.dcsa.mil/is/swft/***

Please follow the instructions on the PSSAR and provide all relevant information as requested. PSSARs with errors will be returned to the submitting organization for correction. Corrected PSSARs for Organization Administrator accounts must be returned to the DCSA CET before a SWFT account can be created. For SWFT accounts requiring WebEnroll functionality, select the 'Access Request Form' under SWFT Resources, then eFP Enrollment (SWFT+) section.

Note: The Annual Cyber Awareness and Personally Identifiable Information training must be completed by the individual requesting the account. The training links are located on the SWFT DCSA website at ***https://www.dcsa.mil/is/swft/***. On the PSSAR, Part 3, numbers 18 and 19 must be checked and the completion date of the training must be filled in.

Access

Step 2: The PSSARs for the Organization Administrators are submitted to the DCSA CET by encrypted e-mail to dcsa.ncr.nbis.mbx.contact-center@mail.mil.

Site Administrators should submit their PSSARs to their Organization Administrator. Industry standard users and WebEnroll users should submit their PSSARs to their Organization or Site Administrator.

Note #1: Direct all questions regarding the PSSAR processing status to the DCSA CET via phone at 1-724-794-5612 or via e-mail to dcsa.ncr.nbis.mbx.contact-center@mail.mil.

Note #2: Once the SWFT account has been created, the DCSA CET will e-mail the Organization Administrator their username, and will request that they call the DCSA CET to obtain a temporary password.

The Organization/Site Administrator will provide the username and temporary password to the requesting user. For WebEnroll users, Organization/Site Administrators are responsible for creating user accounts in both SWFT and WebEnroll.

Step 3: Log in to the SWFT application and use your username and temporary password to register your Public Key Infrastructure (PKI) token. Temporary passwords are only valid for 72 hours.

Access

Step 4: Procure live scan or card scan equipment, if not done already.

The list of FBI certified products and software is available on the FBI website.

Note #1: Organizations that plan to procure and operate their own equipment should obtain access to SWFT prior to procuring any scanning hardware.

Note #2: Any scanning equipment that is intended for producing eFPs must meet the FBI certification guidelines and must be registered with SWFT. SWFT collects and sends all required registration information to the registration authority.

Note #3: The registration and testing of the scanning equipment can be requested and conducted only by an authorized SWFT User. Any other entity that intends to provide electronic fingerprinting services must seek sponsorship from at least one authorized SWFT organization in order to be able to register their scanning equipment. The sponsorship must remain active for as long as such services are provided or offered.

Registration

Step 5: Log in to SWFT and register the fingerprint scanning equipment.

Please note that only the Organization Administrator or Site Administrator has the necessary permissions to register the fingerprint scanning hardware and software. For information on how to register the scanner and software, click the "Help" button in the SWFT application to access the *NBIS-SWFT Scanner Configuration and Registration Guide*. WebEnroll users are required to register scanners in both SWFT and WebEnroll. For information on how to register the scanner and software, click the "Help" button in the SWFT application to access the *NBIS-SWFT Users Guide* under the WebEnroll section.

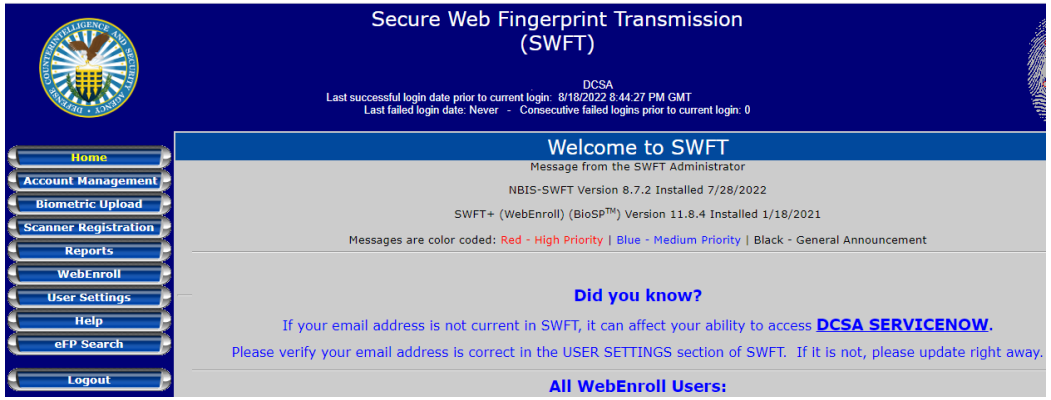
Note #1: Upon completing the entry of the scanner registration information, the Organization Administrator or Site Administrator submits the scanner registration to the SWFT Coordinator by clicking the "Submit" button. The SWFT Coordinator reviews the scanner registration. Registration data that does not pass the validation check is rejected. The Organization Administrator or Site Administrator must then correct and re-submit the registration data. Completed fingerprint scanner registrations are submitted by the SWFT Coordinator to the registration authority for approval.

Note #2: When registering the scanner, ensure that the Transaction Control Number (TCN) Prefix complies with the convention that is outlined in the *NBIS-SWFT Scanner Configuration and Registration Guide*. Each fingerprint scanner and fingerprint card scanner must have its own unique TCN Prefix. The *NBIS-SWFT Scanner Configuration and Registration Guide* can be accessed by clicking the "Help" button in SWFT.

Registration

Step 6: After successful registration of the scanner hardware and software data, the SWFT Coordinator notifies the Organization Administrator or Site Administrator via e-mail that the scanner is ready for testing. The scanner must be properly configured to produce eFP files that comply with EBTS standards and requirements defined by the investigative service providers. Refer to the *NBIS-SWFT Scanner Configuration and Registration Guide* which can be accessed by clicking the "Help" button in SWFT.

Note: It is not necessary to re-register or re-test the scanner workstation separately for each new Org/CAGE Code that the workstation supports. The same applies to a scanner workstation that is being sponsored by an authorized SWFT account holder.



Testing

WebEnroll Users: Skip steps 7 through 9 and follow the instructions in the Scanner Test Guide found under the SWFT Resources, then eFP Enrollment (SWFT+) section on the SWFT DCSA Website for testing new scanners.

Step 7: The Organization Administrator or Site Administrator uploads the test eFP to SWFT and notifies the SWFT Coordinator by email at dcsa.ncr.nbis.mbx.swft@mail.mil after the eFP is successfully uploaded.

The SWFT upload process rejects the test eFP if the device serial number on the eFP does not match the device serial number registered in the SWFT application in Scanner Registration.

Refer to the *NBIS-SWFT Scanner Configuration and Registration Guide* for detailed instructions pertaining to the enrollment and upload of a test eFP. Please note the following before uploading a test eFP to SWFT:

Note #1: The maximum acceptable eFP file size is 1MB for both test and production submissions. If the eFP file size is greater than 1MB, consult the vendor on how to set the scanner resolution and/or file compression to bring the size of the eFP file within 700–1,000KB range.

Note #2: Fingerprint card scanning equipment often exports only the fingerprint images from the paper card. As a result, you may have to re-enter all the biographical data manually. Please contact the appropriate software vendor for information on how your card scanner should be configured to generate eFPs meeting the DCSA FTS and other registration authority standards.

Testing

Step 8: The SWFT Coordinator reviews the uploaded eFP and reports any issues. If errors are identified in the eFP, the SWFT Coordinator works with the Organization Administrator or Site Administrator on resolution. This process will require re-submission of a corrected eFP to SWFT. Verified test eFP files are forwarded to the registration authority for validation.

Note #1: An automated e-mail notification is sent to the Organization Administrator or Site Administrator when the test eFP file has been submitted to the registration authority. The SWFT Coordinator receives notification of the test result via e-mail from DCSA FTS within one to two business days after submission of the test eFP to DCSA FTS.

Note #2: Currently, only DCSA FTS sends a confirmation e-mail to the SWFT Coordinator after a test eFP has been received. This may change in the future for other registration authorities.

Testing

Step 9: For each test eFP submitted to the registration authority, the SWFT Coordinator communicates one of the following possible test results by e-mail to the Organization Administrator or Site Administrator:

Result #1: The test eFP was successfully processed and the scanner/software is authorized to submit eFPs to production.

Result #2: The test eFP was rejected by the Registration Authority.

The SWFT Coordinator will help with resolving the issues with the test eFP. Errors found during the registration authority validation of the test eFP require resubmission of a corrected test eFP to SWFT. Steps 7–9 are repeated until the scanner has been approved for production use by the Registration Authority.

Questions

For any questions or concerns, please contact the DCSA CET at
dcsa.ncr.nbis.mbx.contact-center@mail.mil

Or contact the SWFT Coordinator via email at
dcsa.ncr.nbis.mbx.swft@mail.mil
or ServiceNow at
https://dcsa.servicenowservices.com