DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY - SECURE WEB FINGERPRINT TRANSMISSIONS (DCSA-SWFT)

ACCESS, REGISTRATION, AND TESTING PROCEDURES

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Document Version 4.5

January 2025

DOCUMENT INFORMATION

REQUIRED INFORMATION	DEFINITION
Document Title:	Defense Counterintelligence and Security Agency- Secure Web Fingerprint Transmissions (DCSA-SWFT) Access, Registration, and Testing Procedures
Document ID:	SWFT 1029.U*16
Version:	Version 4.5
Contract #:	HHSN316201200026W
Approval Date:	January 2, 2025
Location:	SharePoint - SWFT Documents\Documentation\SWFT Release 9.6\SWFT Access Registration & Test Procedures
Owner:	DCSA/PEO
Prepared By:	iWorks Corporation
Author:	SWFT Team
Approved By:	Government PM

DOCUMENT HISTORY

Revisions and version changes to this document are recorded within the following table. New versions are published when changes to the document equate to 10 percent or greater of the document's content, or if a change requires immediate implementation. This record is maintained throughout the life of the document.

DATE	VERSION	DESCRIPTION OF CHANGE	NAMES/NOTES
11/29/2018	3.8	SWFT website update	SWF.1029.U*12 / SWFT Team
11/29/2018	3.8	Technical Writer review	SWF.1029.U*12 / TW Team
11/29/2018	3.8	Final Review and delivery	SWF.1029.U*12 / SWFT Team
10/28/2020	3.9	Cover page for SWFT Release 8.6	SWF.1029.U*13 / SWFT Team
12/01/2020	3.9	Technical Writer review	SWF.1029.U*13 / TW Team
12/01/2020	3.9	Final Review and delivery	SWF.1029.U*13 / SWFT Team
03/15/2021	3.9	Update Coversheet	SWF.1029.U*13 / SWFT Team
01/18/2022	3.10	Update release 8.7 changes	SWF.1029.U*14 / SWFT Team
08/23/2022	3.10	Browser updates	SWF.1029.U*14 / SWFT Team
02/20/2023	3.11	Federal Agency updates	SWF.1029.U*15 / SWFT Team
07/17/2023	4.4	Update release 9.0 changes	SWF.1029.U*16 / SWFT Team
01/02/2025	4.5	Update release 9.6 changes	SWF.1029.U*17 / SWFT Team

TABLE OF CONTENTS

1. CONVENTIONS

This guide provides information for the proper use of the Secure Web Fingerprint Transmissions (SWFT) application.

Throughout the document, clickable links, buttons, and names of screen shots are bolded.

This document utilizes hyperlinks for easier navigation. When viewing this document in Microsoft Word, control-click any direct reference to a table, section, or specific number to navigate there instantly.

Helpful hints are printed in *blue italicized font* and are displayed with this  icon.

This guide assumes that the user has a thorough comprehension of using web browsers and browser-based applications, along with an understanding of basic Microsoft Windows file management principles.

The SWFT Access, Registration, and Testing Procedures document is a living document and is subject to revision with project policy changes. Changes to the guide will be managed and controlled.

Important Note:

All users are required to read and accept the rules and terms of use regarding the SWFT application before logging into the system by checking the acknowledgement box on the login page. Below is the text of the Department of Defense (DoD) Notice and Consent banner displayed on the login page.

- You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, Communication Security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (for example, authentication and access controls) to protect USG interests - not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential.

 *All Personally Identifiable Information (PII) data used in this document is fictitious.*

2. ACCESS, REGISTRATION, AND TESTING PROCEDURES (ART) OVERVIEW

The ART provides potential SWFT Users a preview of the procedures necessary for gaining access to SWFT and preparing the electronic fingerprint (eFP) workstation/facility for the use of SWFT.

3. INTRODUCTION

1. SWFT OVERVIEW

Secure Web Fingerprint Transmissions (SWFT) is a Defense Counterintelligence and Security Agency (DCSA) Personnel Vetting system for centralized collection and distribution of electronic fingerprints for applicants requiring investigation services. It is a web-based store-and-forward system for distribution of electronic fingerprints (eFPs), plus an integrated web-based application, WebEnroll, for online capture (also called enrollment) of biographic and biometric data. The Under Secretary of Defense for Intelligence (USD(I)) signed a memorandum on June 22, 2016, directing all Department of Defense (DoD) components to use the Secure Web Fingerprinting Transmissions Plus Enrollment system. DCSA-SWFT and SWFT can be used interchangeably, with SWFT being used within this document.

SWFT eliminates the need for paper-based capture and handling of fingerprints, expedites the investigation services process by reducing invalid fingerprint submissions, provides end-to-end accountability for sensitive Personally Identifiable Information (PII) data, and implements stringent security standards for all electronic transactions.

WebEnroll collates the subject data into standard eFP files and automatically forwards them into SWFT. WebEnroll and Biometric Services Platform (BioSP™) can be used interchangeably, WebEnroll is used within this document.

SWFT ingests eFPs though the user interface and via application-to-application interfaces; eFP files must be produced by certified fingerprint scanner hardware and software that has been registered in SWFT, tested, and approved for production use. There are currently four mechanisms for submitting eFPs to SWFT:

- Send electronic files to SWFT

eFP files can be delivered to SWFT by any one of the following methods:

  - Online Fingerprint File Upload – (User Interface) An operator captures biometric and fingerprint data utilizing an approved capture device and capture software and produces an eFP file. The resulting eFP file is uploaded through the SWFT web application from the Biometric Upload Screen. SWFT does allow for uploading of multiple eFPs at once, but typically in lower volumes such as less than 50 at a time.
  - Online Fingerprint Enrollment – (User Interface) An operator captures biometric and fingerprint data utilizing an approved capture device via WebEnroll. The resulting eFP is automatically submitted to the SWFT application. This option is available only to DoD components participating in the WebEnroll program. *Contact the DCSA Biometric Program Management Team regarding use of the Online Fingerprint Enrollment.*
  - Secure Shell (SSH) File Transfer Protocol (SFTP) – (Application-to-Application Interface) High volume users submit eFPs to SWFT via a Secure File Gateway (SFG) within an SFTP. In this scenario, an organization may have many workstations with approved capture devices and

capture software. The organization collects the eFPs from these workstations (which may number in the hundreds per day) and transmits them via SFG (SFTP) to SWFT. *Contact the DCSA Biometric Program Management Team regarding use of the SFTP transfer.*

- Upload Web Service – (Application-to-Application Interface) A client developed external web application transfers eFPs to SWFT. SWFT is configured with a Representational State Transfer (REST) architectural style, or RESTful web service, where eFPs are programmatically received by SWFT. *Contact the DCSA Biometric Program Management Team regarding use of the Upload Web Service.*

- *eFP Data Verification*
  - The SWFT system validates select data entries in each eFP file before accepting and processing the eFP file. If the eFP does not pass the validation test, the eFP file is not retained in SWFT and a corrected eFP must be resubmitted.
- *Release to Authorized Destinations*
  - The eFP file is securely transmitted from SWFT to the authorized destination(s). The eFP files are deleted from the system when their retention period expires.

2. ACCESS, REGISTRATION, AND TEST (ART) OVERVIEW

Three phases must be completed before cleared organizations can submit production eFPs to SWFT. Appendix A provides an access, registration, and testing process flow diagram.

1. Gaining SWFT access
2. Registering fingerprint scanner or server platform
3. Testing fingerprint scanner or server platform to gain approval for official eFP enrollment

1. SWFT ACCESS

Access to SWFT can be granted to the following users:

- National Industrial Security Program (NISP) cleared organizations
- U.S. Military components and DoD agencies
- U.S. Federal 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 [for example, Common Access Card (CAC), External Certificate Authority (ECA), Personal Identity Verification (PIV) or Personal Identity Verification-Interoperable (PIV-I) credential].

Prior to procuring a fingerprint capture device and software, all new SWFT users first need to complete and submit their Personnel Security System Access Request (PSSAR) package (which includes the PSSAR form, PII training certificate, and Cyber training certificate, completed within the prior 12-month time period) to the appropriate SWFT account administrator.

 *Do not submit PSSARs to the SWFT Coordinator.*

 *PSSARs can be found on the the SWFT DCSA Website at https://www.dcsa.mil/is/swft/.*

All Users accessing SWFT or WebEnroll, go to the DCSA SWFT Website, select the "PSSAR Form" under "SWFT Resources", then "Access Request" section.

Once the user's PSSAR has been processed, the user receives a SWFT username and temporary password from their Site/Organization Administrator. The username and temporary password are used only to register their Smart Card credentials. The temporary password is only valid for 72 hours. Once their selected credential is successfully registered, they only need the Smart Card to log in to SWFT.

Each organization should appoint primary and backup Organization Administrators who are responsible for management of accounts and records affiliated with the Organization. Besides performing administrative tasks such as creating and managing user and lower-level administrative accounts, registering, and managing fingerprint capture devices, etc., the Organization Administrators can also perform all tasks as regular SWFT users.

Larger organizations that have fingerprint processing facilities in multiple locations should consider appointing primary and backup Site Administrators for each location. The Site Administrators are responsible for creating and managing user accounts, registering, and managing fingerprint capture devices for their site, and can also perform functions of a regular SWFT user.

Refer to Appendix C – Roles and Responsibilities for a list of the SWFT user roles and the responsibilities of each user in the ART process.

2. Fingerprint Scanner Registration

The hardware and software used for capturing the biometric and biographic data and producing the eFP must be listed in the Federal Bureau of Investigation (FBI) list of certified products. To prove that the components of the fingerprinting system meet the FBI certification guidelines, the hardware and software must be registered in SWFT, tested, and approved by the Registration Authority.

SWFT provides an online registration process for registering new fingerprint scanners or server platforms and/or updating the registration information of existing fingerprint scanners or server platforms. The SWFT Coordinator monitors and administers the registration process for all fingerprint capture devices and coordinates troubleshooting and test activities leading to the approval of devices for official eFP enrollments.

3. Testing and Approval of Systems for Production

Every fingerprint capture system (live scan, card scan, or server platform) is registered, tested, and approved for production by the registration authority before enrolling official biometric data. The test of the fingerprinting system proves that the system is properly configured and generates eFP files that comply with the FBI Electronic Biometric Transmission Specification (EBTS) and the registration authority specifications. The specifications are available on the FBI website.

The SWFT Coordinators are the point-of-contact (POC) to the Registration Authority. They arrange test sessions with the Registration Authority and assist in verifying and/or resolving issues with the Test eFP files.

1. ACCESS, REGISTRATION, AND TESTING PROCEDURES

This section provides a step-by-step overview of the procedures for obtaining access to SWFT, registering fingerprint scanners or server platforms, and testing these devices for the purpose of submitting production eFPs. If there are any questions related to these procedures, refer to the SWFT User Guide, SWFT Scanner Configuration and Registration Guide, and WebEnroll Users Guide, which are accessible to SWFT account holders by clicking the Help button on the SWFT Welcome screen.

1. OBTAIN SWFT ACCESS

Step 1: Complete the PSSAR form

The Authorized Organization Representative obtains the PSSAR form from the SWFT DCSA website at: https://www.dcsa.mil/is/swft/.

Follow the instructions on the PSSAR and provide the information as requested. PSSARs with errors or missing information are returned to the submitting organization for correction. Verify all the required information on the PSSAR is filled out and correct to ensure the access request is processed without delay.

All applicants for SWFT accounts must provide certificates of completion for training in Security Awareness and safeguarding PII.

A PSSAR that nominates an Organization Administrator must be signed by the organization's Director, Commander (or delegate), or Key Management Personnel (KMP) listed in the Industrial Security Facilities Database (ISFD). Agency delegates must be an O-5/GS-14 (or agency equivalent) or higher.

To receive a SWFT account,

- The DoD applicant must have and maintain a favorable security clearance eligibility of Interim Secret.
- The Federal Agency applicant must have and maintain a minimum investigation level of Public Trust.

 *PSSARs submitted without the Nominating Official's statement regarding duties and signature will not be processed.*

Step 2: Submit PSSAR form

Organization Administrators complete and submit their PSSAR to the Fingerprint Transaction Systems (FTS) System Liaisons by encrypted e-mail to dcsaftsteam@mail.mil. Use of encrypted e-mail for transmitting any Privacy Act Data is required. For any issues with sending encrypted emails, send a non-encrypted email to the FTS System Liaisons without the PSSAR for additional assistance.

Once the SWFT account has been created, the FTS System Liaisons e-mails the Organization Administrator their username and requests that they call the FTS System Liaisons to obtain their temporary password.

Site Administrators complete and submit their PSSAR to their Organization Administrator. Organization Administrators are responsible for creating and managing Site Administrator, standard, and basic (non-privilege) user accounts. The Organization Administrator provides the username and temporary password to the requesting user. The PSSAR should not be submitted to the FTS System Liaisons.

Standard and basic (non-privilege) users complete and submit their PSSAR to their Organization or Site Administrator. Organization/Site Administrators are responsible for creating and managing standard and basic (non-privilege) user accounts. The Organization/Site Administrator provides the username and temporary password to the requesting user. Standard and basic (non-privilege) users should not seek account assistance from or submit the PSSAR to the FTS System Liaisons.

WebEnroll users submit the completed PSSAR to their Organization or Site Administrator. Organization/ Site Administrators are responsible for creating user accounts in both SWFT and WebEnroll. The Organization/Site Administrator provides the username and temporary password to the requesting user. The PSSAR should not be submitted to the FTS System Liaisons.

WebEnroll users should make sure that they have selected the "Enroller" and "Transaction Viewer" roles on the PSSAR form. If WebEnroll users cannot access WebEnroll, contact your Administrator to verify that your WebEnroll account was created.

Do not submit PSSARs to the SWFT Coordinator. The SWFT Coordinator does not process PSSARs. Please send all PSSARs and PSSAR related communication to the FTS System Liaisons at dcsaftsteam@mail.mil or the appropriate Organization/Site Administrator.

Step 3: Log into SWFT

All users need to use their username and temporary password during the first login to SWFT to register their PKI token with their SWFT account. Thereafter, the PKI token is automatically used to authenticate the user to SWFT.

4.2 REGISTRATION OF FINGERPRINT SCANNER OR SERVER PLATFORM

Step 4: Procure fingerprint scanner or server platform equipment

The Authorized Organization Representative procures fingerprint scanner or server platform equipment. The list of FBI certified products and software is available on the FBI website.

Organizations that wish to procure their own equipment should obtain access to SWFT prior to procuring any scanning hardware.

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

Step 5: Register the fingerprint scanning equipment

WebEnroll users are required to register scanners in both SWFT and WebEnroll. Please refer to the below instructions on how to register the scanners in SWFT For instructions on correct setup of WebEnroll functionality, refer to the *WebEnroll Users Guide* in the Help section of the SWFT application under SWFT+ (WebEnroll) User Guides.

Using the credentials obtained in Step 3, the Organization Administrator or Site Administrator logs into SWFT to register their scanner(s). For information on how to register the scanner, click Help in the SWFT application to access the *SWFT Scanner Configuration and Registration Guide*.

The registration process can be initiated only by an administrative user from an organization that is authorized to use SWFT. An organization without access to SWFT that wishes to provide electronic fingerprinting services to authorized users of SWFT must seek sponsorship for their fingerprint system from at least one authorized SWFT user organization. The sponsorship must be maintained active for as long as such services are provided or offered.

IMPORTANT: When registering the scanner, ensure that the Transaction Control Number (TCN) Prefix format matches one of the examples listed in the SWFT Scanner Configuration and Registration Guide. Each fingerprint scanner and fingerprint card scanner must have its unique TCN Prefix, even if multiple devices are managed by the same computer workstation. TCN prefixes for eFPs submitted by service providers on behalf of other organizations do not need to be customized for each client and should remain constant. Click Help in SWFT to access the SWFT Scanner Configuration and Registration Guide.

Upon completing the entry of the fingerprint scanner registration information, the Organization or Site Administrator submits the scanner registration to the SWFT Coordinator by clicking Submit.

IMPORTANT: Be sure to click "Submit" rather than "Save", or the scanner registration will not be processed.

The SWFT Coordinator reviews and validates the fingerprint scanner registration. Scanners that do not pass this validation check are returned to the submitting Organization or Site Administrator for correction. Completed fingerprint scanner registrations are submitted by the SWFT Coordinator to the registration authority for approval.

Step 6: Configure fingerprint scanner or server platform equipment and software

The Organization/Site Administrator receives an e-mail from the SWFT Coordinator confirming the scanner has been registered and authorized for testing by the registration authority. The scanner must be properly configured to produce eFP files that comply with EBTS standards and requirements defined by the investigative service providers. For information on how to configure the scanner, click Help in the SWFT application to access the *SWFT Scanner Configuration and Registration Guide.*

If you are a service provider whose fingerprint scanner or fingerprint card scanner is being sponsored for production use by an authorized SWFT account holder, you do not have to re-register the equipment each time you provide services to another SWFT client.

If you are using WebEnroll, steps 7 through 9 in the following section are not required. Instead, follow the instructions in section 4.4 WebEnroll Testing below. These steps are also available on the DCSA SWFT Website, under eFP Enrollment, then WebEnroll Scanner Test Guide.

For additional configuration and administration tasks necessary for WebEnroll, click Help in the SWFT application and select the "Administrator Guide for WebEnroll SWFT+".

4.3 TEST EFP UPLOAD

Step 7: Submit the Test eFP to SWFT

The Organization or Site Administrator submits the Test eFP to SWFT and notifies the SWFT Coordinator by e-mail at dcsa.ncr.nbis.mbx.swft@mail.mil after the eFP is successfully submitted. The device serial number on the eFP must match the device serial number registered in the SWFT application in Scanner Registration. If the serial numbers do not match, then the Test eFP is rejected. The Organization or Site Administrator must correct the device serial number in Scanner Registration and re-upload the Test eFP.

For instructions pertaining to uploading a Test eFP, click Help in the SWFT application to access the *SWFT Scanner Configuration and Registration Guide.*

Step 8: Test eFP submitted to the registration authority

The SWFT Coordinator reviews the uploaded eFP for errors. If the eFP does not contain errors, the SWFT Coordinator submits the Test eFP file to the registration authority for validation. The Organization or Site Administrator is notified by e-mail when the Test eFP is submitted to the registration authority. The test results are typically received within two business days.

If errors are identified in the eFP, the SWFT Coordinator works with the Organization or Site Administrator to resolve them. Once resolved, submission of a corrected Test eFP to SWFT is required to complete the process and receive final approval.

Step 9: Receive Test Results

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

- "The Test eFP was successfully processed and the scanner is authorized to submit eFPs to production."
- "The Test eFP was rejected by the registration authority." The SWFT Coordinator will provide the reason it was rejected and will assist the Organization or Site Administrator to resolve the issue with the Test eFP. Errors found during the registration authority validation of the Test eFP will require submission of a corrected Test eFP to SWFT. Steps 7, 8, and 9, will be repeated until the scanner has been approved for production use by the registration authority.

4. WEBENROLL TESTING

1. Make sure that your Live Scan or Card Scan device is connected to your workstation.
2. Log into SWFT at https://swft.nbis.mil and navigate to "WebEnroll".
3. Click on WebEnroll from the dropdown menu.
4. Click on New Enrollment, the Biographic Information screen is displayed.
5. Enter Last/First Name: Test, Test <= CRITICAL REQUIREMENT
6. Enter the Date of Birth (must be minimum 18 yrs. old).
7. Enter the Place of Birth (select any from the dropdown list).
8. Enter the Citizenship (select any from the dropdown list).
9. Enter the Gender, Race, Height, Weight, Eyes, and Hair (select any from the dropdown list or type any valid entry).
10. Enter an SSN (must be all 9's). <= CRITICAL REQUIREMENT
    Example: 999999999
11. Enter the Reason Fingerprinted: Test. <= CRITICAL REQUIREMENT
12. Enter the SON (leave default system value or provide any valid entry).
13. Enter the SOI (leave default system value or provide any valid entry).
14. Enter the IPAC/ALC (leave default system value or provide any valid entry).

15. Review all entries and correct as needed.
16. Click the Save and Continue button.
17. Provide all fingerprint images.
18. Click the Save and Continue button.
19. Review all data presented on the page.
20. Click the Complete Enrollment button.
21. Create a ServiceNow ticket at https://dcsa.servicenowservices.com and send notification to the SWFT Coordinator:
    SUBJECT: Web Enroll Test (UNCLASSIFIED)
    MESSAGE: Test submission was completed by: <enter your WebEnroll User ID>.
    Test SSN: <enter the test SSN >
22. SWFT Coordinator reviews the Test submission and sends back results for production approval.

1. OPTIONS FOR SUBMITTING EFPS

2. OPTION ONE: ORGANIZATION UPLOADER

The Organization submits their own eFPs

An organization submits fingerprints for their own personnel, typically associated with the Organization or CAGE (Commercial and Government Entity) Code assigned to their SWFT account. This allows the SWFT user to access detailed SWFT reports that contain PII data for their organization. The SWFT user will be able to generate reports that identify the date and number of eFPs uploaded on behalf of their organization.

The SWFT user/Agency registering the scanner assumes the responsibility of all activities and use of that scanner. All usage should comply with established PII protection and security policies.

2. OPTION TWO: MULTI-SITE UPLOADER WITH LIMITED PERMISSIONS

Service Provider with Limited Permissions Submits Fingerprints on Behalf of another Organization

A Multi-Site Uploader can submit eFPs on behalf of any organization that is registered in the SWFT system. Any SWFT account holder can act as a Service Provider for one or more organizations if the "Multi-Site Uploader" role is enabled for that account. This allows the Service Provider or any other SWFT user with "Multi-Site Uploader" permissions to submit eFPs for other organizations and generate reports that identify eFPs they uploaded on behalf of other organizations, which is useful for billing and accountability purposes.

The DCSA CET Executive Administrators can grant the permission to use the "Multi-Site Uploader" role after receiving a valid PSSAR approved by the appropriate nominating official from the service provider.

Tasks to be completed by Serviced Organizations:

Serviced organizations must obtain at least their own Organization Admin account and have an Organization record created, before seeking services from a Service Provider. An Organization record does not require a fingerprint scanning device to be registered or associated with it. A Serviced organization with an Organization record can maintain their SWFT Org Admin user account to track the fingerprint transactions that were submitted on their behalf by Service Providers.

Verify the service provider that generates the eFPs for your organization has its equipment registered and approved for production by SWFT/DCSA and the registration authority. To confirm the approval

status of the equipment, generate one of the following reports based on the information provided by the Service Provider:

- Report 1: Scanner Registration Status by Hardware Vendor and Serial Number
    a. Obtain the Hardware Vendor and Scanner serial number
    b. Log in to SWFT
    c. Run the "Scanner Registration Status by Hardware Vendor and Serial Number" report accessible via the Reports button on the SWFT menu
    d. The Scanner Registration Status by Hardware Vendor and Serial Number report displays one of the following messages based on the selected hardware vendor and scanner serial number combination:
        i. *"Hardware Vendor" has registered scanner(s)
        ii. *No scanner registration for hardware vendor "HW Vendor" with serial number "#####"
- Report 2: Scanner Registration Status by Org/CAGE Code
    a. Obtain the Org/CAGE Code from the Service Provider
    b. Log in to SWFT
    c. Run the "Scanner Registration Status by Org/CAGE Code" report accessible via the Reports button on the SWFT menu
    d. The "Scanner Registration Status by Org/CAGE Code report displays one of the following messages based on the selected Org/CAGE Code:
        iii. * "Organization Name" has registered scanner(s)
        iv. * There is at least one registered scanner
        v. * No scanner registration for Org/CAGE Code of "Org/CAGE Code"

Refer to the *SWFT Administrator Guide* and *SWFT Scanner Registration and Configuration Guide* for further information pertaining to SWFT reports. (SWFT Guides are only available to SWFT account holders.)

3. OPTION THREE: MULTI-SITE UPLOADER WITH FULL PERMISSIONS

A Service Provider Acts with Full Permissions 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 separate PSSAR approved by the appropriate nominating official from the serviced organization.

4. OPTION FOUR: 3RD PARTY SERVICE PROVIDER

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

Third party service providers must have their own hardware/software equipment, which has been registered, tested, and approved for SWFT production under their organization. A 3rd party service provider must also be vetted to offer fingerprint services to DoD and U.S. Federal Agency clients.

The "Fingerprint Service Providers" list, published on the SWFT DCSA website, lists DCSA vetted 3rd party service providers. Some service providers have offices in multiple geographical areas.

Organizations intending to offer their fingerprint services to the DoD and/or Federal Agency communities on the SWFT DCSA website should contact the SWFT Coordinator for qualification criteria and to initiate the vetting process.

The SWFT user/Agency registering the scanner assumes the responsibility of all activities and use of that scanner. All usage should comply with established PII protection and security policies.

1. SERVER PLATFORM FINGERPRINT SYSTEMS

Server platform fingerprint systems typically involve two components:

1. One or more fingerprint scanning devices
2. Server hardware and software 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.

Additional scanning devices that communicate with an approved server platform system must be registered in SWFT, but do not have to be tested. Fingerprint scanning devices that connect to an approved server platform system must include the server platform ID that has already been tested and approved for production by SWFT. On the scanner registration form, the user must select the Device Type "Scanner" and the Operation Mode "Server Platform" when registering the scanner.

For WebEnroll users going through the server platform, when registering the scanners as scanner/server platforms, enter the scanner serial number from the scanner device in the scanner serial number field and enter "BIOSP-SWFT" in the Platform ID field.

1. RE-REGISTRATION AND RE-TESTING

All fingerprint scanner equipment must be re-registered and re-tested under the following circumstances:

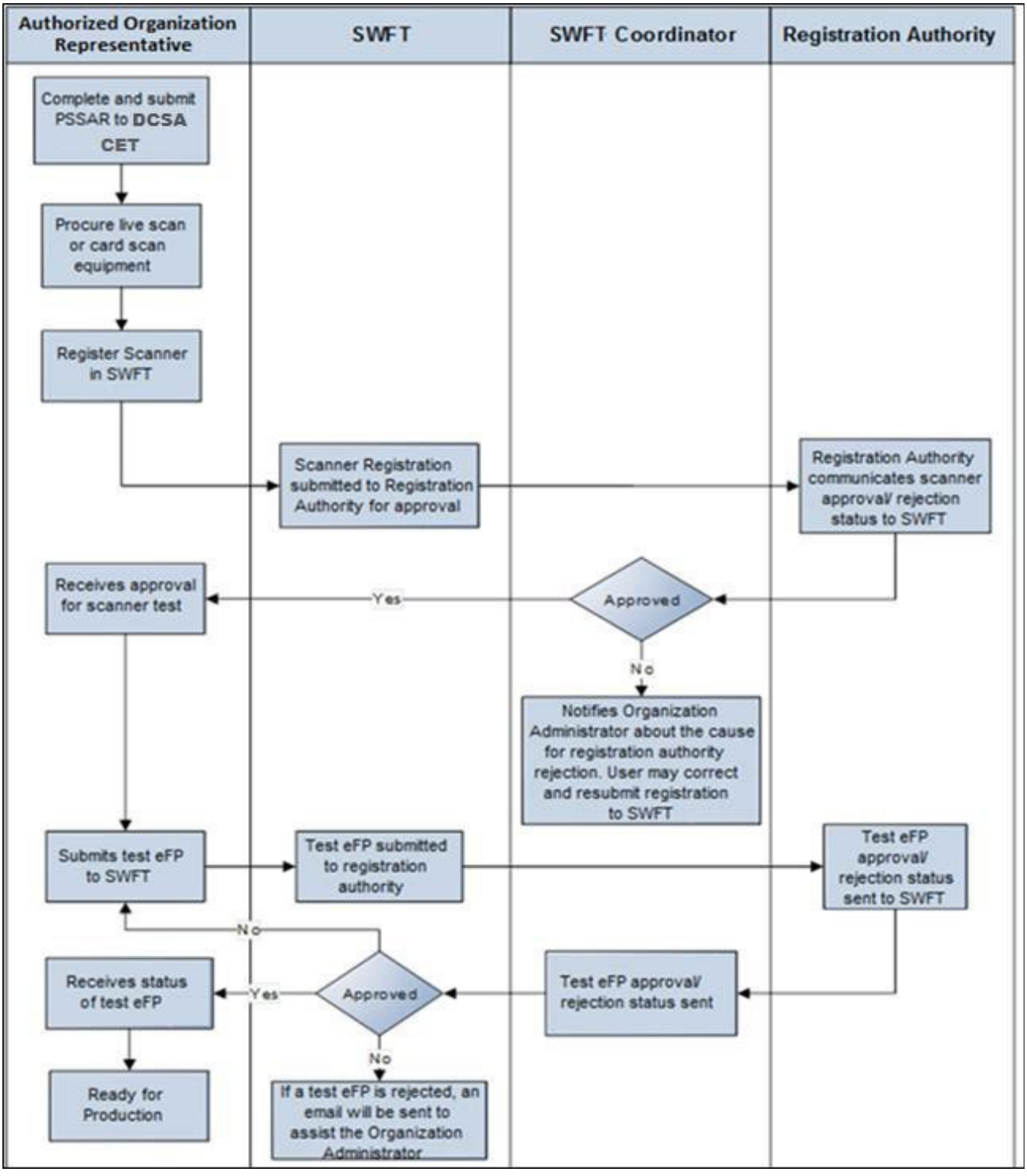
- Any part of the system is replaced (laptop and/or scanner)
- A hardware component is repaired or replaced
- A software upgrade, replacement, or configuration change is performed
- Equipment has been transferred to a new building

Step 1: Edit the pertinent entries on the Scanner Registration screen. The Organization or Site Administrator is required to enter the reason for re-registration and re-testing in the comments section (for example, "*Scanner must be re-registered and re-tested due to software upgrade*").

Step 2: The Organization or Site Administrator submits the form to the SWFT Coordinator by clicking Submit. The scanner registration status is changed to Pending Re-Approval after the scanner changes have been submitted.

Step 3: Continue from section 4.2, Step 6: Configure fingerprint scanner or server platform within this document.

APPENDIX A. SWFT ACCESS, REGISTRATION, AND TEST PROCESS FLOW



APPENDIX B. REFERENCES

Note: If there are connection issues with any of the links listed below, copy, and paste the link into your Web browser to access the reference information.

SWFT DCSA Website

https://www.dcsa.mil/is/swft/

Personnel Security System Access Request (PSSAR) DD Form 2962

https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2962v2.pdf

Cyber Awareness Training

https://www.dcsa.mil/Portals/91/Documents/IS/SWFT/Access%20Request/Training_Requirements_SWFT_Accounts.pdf

PII Training

https://www.dcsa.mil/Portals/91/Documents/IS/SWFT/Access%20Request/Training_Requirements_SWFT_Accounts.pdf

Digital Encryption Instructions

https://www.dcsa.mil/Portals/91/Documents/IS/DISS/DCSA_Contact_Center_Encryption_v1-2.pdf

APPENDIX C. ROLES AND RESPONSIBILITIES

User Role	Responsibility
Basic (Non-Privilege) SWFT User	Requests access, sends completed PSSAR to their Organization/Site Administrator Generates limited reports Submits eFPs
Standard SWFT User	Request Access, send completed PSSAR to your Organization/Site Administrator Generate reports Submit and review eFPs
Organization Administrator (Administrative User)	Process PSSARs for users Manage user and site accounts Create and maintain scanner registration Grant Multi-Site Uploader permissions to their users
Site Administrator (Administrative User) **(Actions are performed only for users and scanners assigned to the Site)**	Process PSSARs for users Manage user accounts Create and maintain scanner registration
SWFT Coordinator (Privileged User)	Manages the scanner registration process Coordinates the scanner test Acts as the POC for communication between the Registration Authority and Organization/Site Administrators
Executive Administrator	Process PSSARs to create accounts for Organization Administrators only Grant eFP Uploader, Multi-Site Uploader and Web Enroller permissions to Organization Administrators
Registration Authority	Verify device hardware, software, and configuration compliance with EBTS standards Provide verification to SWFT Coordinator once an eFP has been received; this is currently only for Fingerprint Transaction Systems (FTS)
Service Provider with limited permissions	Submit eFPs on behalf of other organizations
Service Provider with full permissions	Submit eFPs on behalf of other organizations Generate reports
Serviced Organization **(SWFT Account is recommended but not required)**	Verify Service Provider has registered equipment Send eFPs to Service Provider to be submitted Submit eFPs for their organization