

# *Defense Manpower Data Center*

---

Personnel Security and Assurance



## **Secure Web Fingerprint Transaction (SWFT) Frequently Asked Questions**

**Version 1.0**

July 20, 2016

Contract Number: GS00Q09BGD0027

Task Order: GST0313DS0018

SWF.1084.U\*2

Prepared by

  
**Hewlett Packard**  
Enterprise



# REVISION HISTORY

Date	Version Number	Section	Comments	CM #	Name
6/13/2016	1.0	All	Initial draft	SWF.1084.U*2	SWFT Team
7/05/2016	1.0	All	Technical Writer review	SWF.1084.U*2	TW Team
7/20/2016	1.0	All	Final Review and delivery	SWF.1084.U*2	PSA Systems Support Team

*Note: The controlled master of this document is available on-line. Hard copies of this document are for information only and are not subject to document control.*

# DOCUMENT INFORMATION

Required Information	Definition
Document Title:	Personnel Security/Assurance (PSA) Systems Support Secure Web Fingerprint Transaction (SWFT) Frequently Asked Questions
Document ID:	SWF.1084.U*2
Version:	Version 1.0
Approval Date:	July 20, 2016
Location:	StarTeam – SWFT Documentation\SWFT Frequently Asked Questions
Owner:	PSA Systems Support Team
Author:	PSA Systems Support Team
Approved by:	PSA Systems Support Team

### **GOVERNMENT PURPOSE RIGHTS**

*The Government's rights to use, modify, reproduce, release, perform, display, or disclose these technical data are restricted by paragraph (b)(2) of the Rights in Technical Data-Noncommercial Items clause contained in the DMDC PSA Systems Support contract GS00Q09BGD0027. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings.*



# Secure Web Fingerprint Transaction (SWFT) Frequently Asked Questions

## Contents

**Index**..... 1

**Questions about Access, System Requirements, and User Guide** ..... 1

1. Who can use SWFT?.....1

2. How do I obtain a SWFT account? .....1

3. What are the minimum security requirements for obtaining a SWFT account?.....1

4. Where can I find the Personnel Security System Access Request (PSSAR) form? .....2

5. How recent must the training certificates that I submit with my PSSAR be?.....2

6. Can I e-mail PSSARs to the SWFT Helpdesk? .....2

7. How often must I log into my account in order to avoid account suspension or termination?....2

8. As an Organization or Site Administrator, how do I reinstate a user who has had his or her account terminated due to 45 days of inactivity? .....2

9. What are the system requirements for SWFT? .....2

10. Does an Organization need to have a fingerprint scanner before they can obtain a SWFT account?.....3

11. Is there a User Guide for the SWFT system? .....3

12. My Organization will be utilizing another cleared Organization/Third Party Vendor’s equipment for creating eFP files. Which part of the Access, Registration, and Testing Procedures is relevant for our situation?.....3

**Questions about the Equipment**..... 3

13. What type of fingerprint scanner can be used? .....3

14. What are OPM’s requirements for scanner configuration and settings? .....3

- 10 rolled impressions .....4
- 1 Plain Left and Right Simultaneous Four Finger Impressions .....4
- 1 Plain Left and Right Thumb Impression .....4

15. My Organization is a Third Party Vendor whose fingerprint scanner is being sponsored for production use by a cleared DoD contractor. Will I have to re-register the same fingerprint scanner each time I provide services to other authorized SWFT Users? .....4

16. My Organization will be utilizing a cleared Organization/Third Party Vendor’s equipment for creating eFP files. Will they be able to submit eFPs on our behalf?.....4

17. What is the policy for getting server-based/web-based fingerprint systems registered and tested? .....5

18. What is the timeline for scanner registration and approval?.....5

19. Can I submit eFPs to the Authorized Destination if I never submit a Test eFP?.....5

**Questions about the Fingerprints**..... 6

20. Do the eFPs ever get deleted? .....6

21. Are both rolled fingerprints and flat fingerprints accepted?.....6

22. How are the fingerprint files matched with the Electronic Questionnaires for Investigations Processing (e-QIP) submission? .....6

23. What is the difference between the Transaction Control Number (TCN) and TCN Prefix? .....6

**FOR OFFICIAL USE ONLY**



- 24. What information has to match in JPAS/e-QIP and e-fingerprint to make the clearance process go through most efficiently?.....6
  - 25. Does the investigation number need to be included in the eFP file?.....6
  - 26. What data is entered in the Social Security Number (SSN) field if a person is a Foreign National?.....7
  - 27. Can the SWFT Coordinator change biographic information that was entered incorrectly in an eFP file?.....7
  - 28. My eFP's processing is taking a long time. How can I find out why?.....7
-



## Index

Topic	Question Number
Acceptable fingerprint types	20
Access	1, 2, 9
Account Policies	3, 6, 7
Account Reinstatement	7
Deleting eFPs	19
Documentation	10
e-QIP	21, 23
Editing eFPs	26
eFP Submission and Status	28
Foreign Nationals	25
Investigation Numbers	24
JPAS	23
Obtaining SWFT Account	1
PSSAR	4
Record Retention	18
Scanner Registration Process	13, 17, 18
Scanner Types Supported	12
Server-based Systems	16
System Requirements	8
TCN	22
Third Party Providers	11, 14, 15
Training Requirements	5

## Questions about Access, System Requirements, and User Guide

### 1. Who can use SWFT?

**ANSWER** – SWFT serves cleared companies listed in the Industrial Security Facilities Database, and several Department of Defense (DoD) Commands. Cleared companies and DoD Commands can use SWFT to submit electronic fingerprint files for applicants requiring a background investigation for a personnel security clearance.

### 2. How do I obtain a SWFT account?

**ANSWER** – Please refer to the SWFT Access, Registration and Testing Procedures. The document is available at <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>. Click on the “Access, Reg, and Testing Guide” link in the “Access Request” section of the PSA SWFT Web page.

### 3. What are the minimum security requirements for obtaining a SWFT account?

**ANSWER** – At a minimum, a completed and favorably adjudicated Tier 3 investigation and

**FOR OFFICIAL USE ONLY**



interim secret eligibility are required for a SWFT account. Applicants should not submit a Personnel Security System Access Request (PSSAR) form until they have been granted at least an Interim Secret Clearance.

#### **4. Where can I find the Personnel Security System Access Request (PSSAR) form?**

**ANSWER** – The document is available at: <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>. Click on the “PSSAR Form” in the “Access Request” section.

#### **5. How recent must the training certificates that I submit with my PSSAR be?**

**ANSWER** – In order to receive a SWFT account, training certificates that are less than 12 months old must be submitted with your PSSAR form for the Cyber Security Awareness/Information Assurance (IA) and Personally Identifiable Information (PII) courses.

#### **6. Can I e-mail PSSARs to the SWFT Helpdesk?**

**ANSWER** – No, SWFT PSSARs must be submitted directly to the Defense Manpower Data Center (DMDC) Contact Center at: **dmdc.contactcenter@mail.mil**.

#### **7. How often must I log into my account in order to avoid account suspension or termination?**

**ANSWER** – Users must log into their accounts every 30 days in order to avoid account suspension. Accounts that are not accessed within 45 days of the last login will be terminated. Suspended accounts can be unlocked by Site/Organization Administrators. Terminated accounts will require a new PSSAR to be submitted to your Site/Organization Administrator. Site/Organization Administrators must contact the Executive Administrator at the DMDC Contact Center, if they require assistance with their account.

#### **8. As an Organization or Site Administrator, how do I reinstate a user who has had his or her account terminated due to 45 days of inactivity?**

**ANSWER** – If a SWFT User in your Organization has had their account terminated, you will need to create a new account for that user once you have received a completed PSSAR from that user. You will not be able to reuse the user’s previous username.

#### **9. What are the system requirements for SWFT?**

**ANSWER** – SWFT is entirely web based. Therefore, the only requirement is internet access and a compatible web browser. SWFT currently supports only Microsoft® Internet Explorer® 9.0 or above. Other browsers may work as well. Optionally, in order to be able to upload multiple electronic fingerprints (eFPs) at a time, Adobe Flash Player® 9.0.24 or higher must be installed and enabled. A free download is available at: <http://get.adobe.com/flashplayer/>. Prior to installing Adobe Flash Player® please check your Organization’s Information Technology (IT) policy.



**10. Does an Organization need to have a fingerprint scanner before they can obtain a SWFT account?**

**ANSWER** – No, your Organization does not have to own or sponsor any scanning devices in order to obtain a SWFT account. After obtaining the account, please log into SWFT at least once every 30 calendar days so that your account does not expire.

**11. Is there a User Guide for the SWFT system?**

**ANSWER** – A User Guide is available online to the users after logging into the SWFT web application. Click the “Help” button that is available on each web page. The User Guide is For Official Use Only (FOUO), and is not available to the general public.

**12. My Organization will be utilizing another cleared Organization/Third Party Vendor’s equipment for creating eFP files. Which part of the Access, Registration, and Testing Procedures is relevant for our situation?**

**ANSWER** – If your Organization will be only submitting the eFPs, then only the “Access” section of the SWFT “Access, Registration, and Testing Procedures” will be relevant to your situation. The “Registration and Testing” sections are not applicable as your Organization will be utilizing another Organization’s/Third Party Vendor’s fingerprint scanning system.

However, your Organization must verify that the Organization/Third Party Vendor that will generate the eFPs for you had their equipment registered and approved for production with SWFT. Obtain the Org/CAGE Code from the Organization/Third Party Vendor, then log into the SWFT system at: <https://swft.dmdc.mil>, and run the “Scanner Registration Status by Org/CAGE Code” report in the Reports section. You can also run a similar report if you know the manufacturer and serial number of their scanning device or devices.

## Questions about the Equipment

**13. What type of fingerprint scanner can be used?**

**ANSWER** – The Federal Bureau of Investigation (FBI) maintains a list of products certified as tested and compliant with the FBI's Next Generation Identification (NGI) initiatives and Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications (IQS). The list of FBI certified products is available on the FBI Biometric Specifications (BioSpecs) website under Certifications: <https://www.fbibiospecs.cjis.gov/Certifications>. SWFT Users may choose to acquire any certified product, depending on their actual need.

**14. What are OPM’s requirements for scanner configuration and settings?**

**ANSWER** – For information regarding fingerprint requirements and specifications please refer to "Requesting OPM Personnel Investigations" dated April 2012, which can be found on the OPM website using the following menu options or URL:

MENU: OPM.gov>Investigations>Background Investigations> Requesting OPM Personnel Investigations

URL: <https://www.opm.gov/investigations/background-investigations/requesting-opm-personnel-investigations/>

**FOR OFFICIAL USE ONLY**



The Office of Personnel Management (OPM) only accepts Type-4 fingerprint images for electronic submission, which consist of;

- 10 rolled impressions
- 1 Plain Left and Right Simultaneous Four Finger Impressions
- 1 Plain Left and Right Thumb Impression

If you have additional questions regarding OPM's requirements for eFPs, please e-mail: [livescanauthorization@opm.gov](mailto:livescanauthorization@opm.gov). Information regarding FBI system requirements and approved devices can be found at the FBI BioSpecs website: <https://www.fbibiospecs.cjis.gov/>.

**15. My Organization is a Third Party Vendor whose fingerprint scanner is being sponsored for production use by a cleared DoD contractor. Will I have to re-register the same fingerprint scanner each time I provide services to other authorized SWFT Users?**

**ANSWER** – Fingerprint scanning workstation or server-based scanning systems have to be registered and tested only once. They do not have to be re-registered or re-tested again before being able to service other client companies. Please provide to your customers the manufacturer and serial number of your scanners, or provide them your Org/CAGE Code or the Org/CAGE Code of the Organization that sponsored the registration of your devices so that your customers can verify in SWFT that your equipment has been registered and approved for use. Please note that any change in your system that could affect the quality or contents of electronic fingerprint files (that is, software patches or upgrade, hardware replacement, scanner relocation, and so on) requires the equipment to be retested.

**16. My Organization will be utilizing a cleared Organization/Third Party Vendor's equipment for creating eFP files. Will they be able to submit eFPs on our behalf?**

**ANSWER** – Yes, another Organization that already has a SWFT account can submit eFPs on your behalf. There are two available options which are detailed in the SWFT Access, Registration and Testing Procedures document available at: <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>.

***Option 1: Service Provider Acts with Full Privileges on Behalf of Another Organization***

A Service provider must have its own SWFT account associated with one or more Org/CAGE Codes from other Organizations (for example, serviced Organizations that are seeking fingerprint services from the service provider). This grants the SWFT account that acts as a service provider the permission to submit eFPs on behalf of other Organizations, and also to access all detailed SWFT reports and PII data as if that account holder was registered directly with each serviced Organization.

Each request for adding additional Org/CAGE Codes to an existing SWFT account requires a separate PSSAR approved by the appropriate nominating official from the Organization that is seeking the fingerprint services from the service provider. Serviced Organizations should maintain their own SWFT account and monitor the progress of their eFP submissions.

**FOR OFFICIAL USE ONLY**



**Option 2: Service Provider Acts with Limited Privileges on Behalf of Another Organization**

Any SWFT account holder can act as a service provider for one or more other Organizations if a “Multi-Site Uploader” role is enabled for that account. This allows the service provider to submit eFPs for another Organization, but will not permit accessing detailed SWFT reports and PII data for any of the serviced Organizations. Serviced Organizations must obtain their own SWFT account before another Organization (for example, the service provider) can submit eFPs on their behalf.

Organizations are strongly encouraged to enter into a service agreement that will address handling and protection of the PII data.

SWFT Executive Administrators (that is, DMDC Call Center agents) grant the permission to use the “Multi-Site Uploader” role after receiving a valid PSSAR form approved by the appropriate nominating official from the service provider Organization. Serviced Organizations must maintain their own SWFT account and monitor the progress of their e-fingerprint submissions.

**17. What is the policy for getting server-based/web-based fingerprint systems registered and tested?**

**ANSWER** – Server-based/web-based fingerprint systems typically involve two components: 1) One or more fingerprint scanning devices; 2) Server that integrates fingerprint images and biographic data and generates the electronic fingerprint file.

Multiple scanning devices can be connected to a single server. At least one scanner-server pair must be registered and tested with SWFT/RA (Registration Authority). The registration must prove that the hardware and software components in the server-based/web-based system meet the FBI certification guidelines. The test of the scanner-server pair must prove that the system is properly configured and generates electronic fingerprint files that comply with the FBI Electronic Biometric Transmission Specification (EBTS) and OPM/RA specifications.

Additional scanning devices that communicate with the server must be registered, but do not have to be tested. Scanning devices that will connect to an already registered and tested server-based system must include in the registration form a reference to the registered scanner and server.

**18. What is the timeline for scanner registration and approval?**

**ANSWER** – It usually takes less than three weeks to complete the scanner registration process and receive approval to operate in the production environment.

**19. Can I submit eFPs to the Authorized Destination if I never submit a Test eFP?**

**ANSWER** – All scanners must be tested in SWFT before they can be used to capture eFPs, unless you are using a server-based system, as explained in question 16. Refer to the Access, Registration, and Test Guide on the PSA website for additional information on the scanner testing process.



## Questions about the Fingerprints

### 20. Do the eFPs ever get deleted?

**ANSWER** – Yes, after each eFP is released to the Authorized Destination, the eFP is deleted from the SWFT database after a set time span in accordance to National Archives and Records Administration (NARA).

### 21. Are both rolled fingerprints and flat fingerprints accepted?

**ANSWER** – Only rolled fingerprints are accepted.

### 22. How are the fingerprint files matched with the Electronic Questionnaires for Investigations Processing (e-QIP) submission?

**ANSWER** – The Facility Security Officer (FSO) who initiates the Joint Personnel Adjudication System (JPAS)/e-QIP submission for the Personnel Security Management Office for Industry's PSMO-I approval must select "I" in the Federal Investigations Processing Center (FIPC) field. This triggers a mechanism that delivers necessary e-QIP data to SWFT where they can be matched with the same type of data obtained from the e-Fingerprint file.

### 23. What is the difference between the Transaction Control Number (TCN) and TCN Prefix?

**ANSWER** – The TCN must be unique for each fingerprint transaction, and consists of the TCN Prefix and TCN Suffix. The TCN Prefix remains constant, while TCN Suffix is unique in each fingerprint transaction.

Refer to the Scanner Configuration and Registration Guide, which is accessible through the SWFT Application in the Help Files. The Scanner Configuration and Registration Guide is FOUO, and is not available to the general public.

### 24. What information has to match in JPAS/e-QIP and e-fingerprint to make the clearance process go through most efficiently?

**ANSWER** – To ensure that request for investigation is processed efficiently, it is important that the personal identification information in the subject's JPAS/e-QIP record match with the same information contained in the e-fingerprint. The following match criteria apply:

- SUBJECT NAME
  - **Last Name:** e-fingerprint and e-QIP must match exactly
  - **First Name:** e-fingerprint and e-QIP must match exactly
  - **Middle Name:** Minor difference/discrepancy may be acceptable (that is, Marcie Gail Smith in e-QIP versus M. Gail Smith or Marcie G. Smith in e-fingerprint)
- SOCIAL SECURITY NUMBER - Must match exactly
- DATE OF BIRTH - Must match exactly

### 25. Does the investigation number need to be included in the eFP file?

**ANSWER** – The e-QIP request Identification (ID) does not have to be listed on the fingerprint file. OPM searches for a matching e-QIP case using the Social Security Number (SSN) and other

**FOR OFFICIAL USE ONLY**



subject identifiers.

**26. What data is entered in the Social Security Number (SSN) field if a person is a Foreign National?**

**ANSWER** – Enter all 9s, all 0s, or all 9s with the last digit being a 0.

**27. Can the SWFT Coordinator change biographic information that was entered incorrectly in an eFP file?**

**ANSWER** – The SWFT Coordinator is unable to change any information contained in eFP Files once they are uploaded to SWFT. If biographic information needs to be updated, the subject will need to be reprinted.

**28. My eFP's processing is taking a long time. How can I find out why?**

**ANSWER** – Any differences in fields like Name, SSN, DOB, or POB between the submitted eFP and the e-QIP in JPAS can cause delays. If the eFP has already been uploaded into SWFT, you can check for discrepancies by running the eFP- eQIP Discrepancy report. Do this by clicking the Reports button in the left-hand column and selecting the eFP- eQIP Discrepancy report from the dropdown. Refer to the SWFT User Guide for details on generating reports. The User Guide is available online to the users after logging into the SWFT web application. Click the "Help" button that is available on each web page. The User Guide is FOUO, and is not available to the general public.

To prevent future delays, before submitting the eFP to SWFT, check the eFP to be submitted against JPAS to ensure there are no discrepancies in any fields (such as name, SSN, or DOB).