Defense Security Service

e-QIP Signature Page and Electronic Fingerprint Guide for In-Process Facilities

Version 1.0
February 2014

Issuing Office: **Defense Security Service**
Russell-Knox Building
27130 Telegraph Rd
Quantico VA 22134

Table of Contents

Electronic Fingerprint Submission

The purpose of this section is to outline the options available for companies that are in-process for a facility clearance (FCL) to submit electronic fingerprints. Cleared companies should refer to the eFingerprints-DSS Guide for guidance.

By memorandum dated July 29, 2010, the Under Secretary of Defense for Intelligence issued a requirement for Department of Defense (DoD) components to transition to electronic capture and submission of fingerprint images in support of all background investigations by December 31, 2013 (e-Fingerprint memo).

The Secure Web Fingerprint Transmission (SWFT) website enables industry users to upload electronic fingerprints and demographic information for applicants requiring a background investigation for a personnel security clearance. The SWFT system eliminates the manual paper process (hardcopy fingerprints), expedites the clearance process, and provides end-to-end accountability for Personally Identifiable Information (PII) data.

Electronic Fingerprint Deployment Options

Companies that are in-process for an FCL do not meet the minimum requirements to apply for a SWFT account, as one of the requirements is for the facility to hold an active FCL. The following options offer alternatives for in-process facilities. Please note the fingerprint capture options are the same for both in-process and cleared facilities. Only the SWFT fingerprint submission step is different. As an in-process facility, the DSS Facility Clearance Branch (FCB) can assist you with SWFT submission once you have obtained your electronic fingerprint files. Cleared companies are required to establish their own SWFT account and monitor their own submissions.

Regardless of capture and submission method, fingerprint submission is a 2-step-process.

Step 1: Fingerprint Capture – A subject's fingerprints are captured electronically or using ink and FD-258 fingerprint cards. The subject's PII is recorded within the electronic file or written on the FD-258 fingerprint card. Inked fingerprint cards must be converted to electronic fingerprint files.

Step 2: Fingerprint Submission – A subject's electronic fingerprint file is submitted to the Office of Personnel Management (OPM) via SWFT.

Option A: Submit Electronic Fingerprint File to FCB for Submission via SWFT

Step 1: Fingerprint Capture – A company, Government Contracting Activity (GCA), law enforcement office, or third party vendor that uses Federal Bureau of

Investigation (FBI) Integrated Automated Fingerprint System (IAFIS) Certified fingerprint capture or scanning equipment but does not have a SWFT account captures a subject's fingerprints and saves the file in the required format to meet SWFT, OPM and FBI standards. The electronic fingerprint file is provided to the subject using an agreed upon file transfer methods.

Step 2: Fingerprint Submission – The subject sends the file via the AMRDEC Safe Access File Exchange (SAFE) web application to FCB, who will submit it via SWFT. Electronic fingerprint files must be sent via encrypted channels. Instructions for using SAFE to securely transmit files to FCB are provided in Appendix B: Submitting Signature Pages and Electronic Fingerprint Files to FCB.

Option B: Submit Electronic Fingerprint File via Third Party SWFT Account

Combined Step 1 and Step 2: *Fingerprint Capture and Submission* – Electronic fingerprints may be captured and submitted via SWFT by a cleared company or an approved e-Fingerprint Service Providers that has both FBI IAFIS Certified fingerprint capture or scanning equipment and access to SWFT. Please note that not all approved e-Fingerprint Service Providers have access to SWFT. Check with the provider before scheduling an appointment. If the eFingerprint Service Provider you wish to use does not have access to SWFT, you may use them to complete Step 1: Fingerprint Capture and use option A to complete Step 2: Fingerprint Submission. If a company is not able to utilize one of the above options, contact FCB at occ.facilities@dss.mil.

It is extremely important that you confirm with the organization that will complete the Fingerprint Capture that they can transmit the electronic file to you or to OPM via SWFT. Electronic Fingerprint Files cannot be transmitted directly to the FBI.

Signature Pages

After completing all sections of the Personnel Security Questionnaire (PSQ) in e-QIP and certifying answers, applicants are required to complete several additional steps in order to properly submit the PSQ for processing. All steps are REQUIRED and the investigation request will not be submitted until these steps are completed:

1. Print or save an Archival Copy of the entire form.

The Archival Copy of your PSQ should be provided to your FSO to retain in your personnel file until your investigation is complete. It is also highly recommended that you also retain a copy for your records.

2. Print the following four (4) signature forms that you will sign and send to your sponsoring agency (DSS FCB):
    - Certification Page (e-QIP Document Type CER)
    - Authorization for Release of Information (e-QIP Document Type REL)
    - Authorization for Release of Medical Information (e-QIP Document Type MEL) – Required if you answered "Yes" to Question 21.
    - Fair Credit Reporting Disclosure and Authorization (e-QIP Document Type FCR)

You should save a blank copy of the signature pages in case new copies are required as this is the most frequent reason for e-QIP rejections.

In e-QIP Step Four: Upload or Fax Attachments, select No to indicate that you do not want to add any attachments.

3. Release and transmit the investigation request to the requesting agency

4. Send signature pages to sponsoring agency (DSS FCB)

Scan your signed signature pages and follow the instructions in Appendix B: Submitting Signature Pages and Electronic Fingerprint Files to FCB to securely transmit them to FCB through SAFE. If this option is not possible, forms can instead be faxed to FCB at 571-305-6922.

Important! You will not be able to access your investigation forms after you click "Release Request/Transmit to Agency." Be sure you have printed and/or attached all required forms, including signature forms, before clicking "Release Request/Transmit to Agency."

FCB will carefully review your submitted form. In the event your information or attachments are incomplete, we may contact you for additional action. The most common reasons for rejection are below.

Common Errors

Signature Pages

Dates are illegible – The correct date (the actual date that forms are signed) should be written or typed entirely within the box provided in neat, legible number. If a mistake is made, do not mark over the existing number. Instead, reprint the forms and re-sign and date clean copies. If this option is not available, make a single dark line through the existing date, re-write the date in neat, legible numbers, and initial the change.

Signature issues – The signature must not cross through any text on the form. The signed name should match the typed name that was automatically populated on the form. If the name is incorrect, you must contact FCB to have your PSQ rejected to you to make the correction within the form.

Extraneous markings – Do not make any extraneous marking on the forms. The name, other names used, phone number, and address boxes are automatically populated with the data you provided in the PSQ. If this information is incorrect, you must contact FCB to have your PSQ rejected for corrections.

Form clarity – All text must be clearly legible with no lines or marking through any text.

PSQ Answers

References – Complete information, including name, address, and telephone number must be provided for all residence and employment verifiers and personal references.

Employment – The company you are submitting the PSQ for must be listed as current employer.

Depending on when errors are identified and type of error, your FCB POC may either contact you to provide corrected signature forms or information via SAFE or return your PSQ in e-QIP.

In the event you are contacted to make corrections to a PSQ that has been returned to you via e-QIP, you will need to:

- Log into e-QIP
- Review the details of the request and make corrections via the e-QIP system
- Re-certify and print a new archival copy of the form
- Re-release your form to the agency
- Print and sign new signature pages (Investigation Request ID on the signature pages must match the current Investigation Request ID) and provide to FCB via SAFE

Once the investigation has been scheduled, you may be contacted by an investigator to schedule your personal interview, if required. In the event an interview is necessary, you will be required to provide photo identification, such as a valid state driver's license. You may be required to provide other documents to verify your identity, as instructed by your investigator.

Handling Personally Identifiable Information

Safeguarding PII is the responsibility of every Federal agency and all users of Federal information and information systems. As a user of DoD information systems, regardless of whether they are military, civilian, or a contractor personnel, they are responsible for protecting PII from unauthorized use or disclosure, as required by Federal laws and DoD regulations. Electronic fingerprint files and signature pages must be sent via encrypted channels when transmitted over the Internet. The preferred method of transmission is via SAFE. Instructions for submitting files containing PII to FCB using SAFE are provided in Appendix B: Submitting Signature Pages and Electronic Fingerprint Files to FCB.

Appendices

Appendix A: Frequently Asked Questions

QUESTIONS AND ANSWERS: The following questions and answers are in response to queries or anticipated queries regarding the submission of signature pages and electronic fingerprints for personnel security investigations:

Q: How long does the PCL process take?
A: The PCL process timeline varies depending on a number of factors, including investigation level and background complexity. In order to speed up the process, you should ensure that all PSQ answers are complete and accurate (reviewing the Common Errors section will help you to avoid the most frequent causes for rejection of a PSQ) and submit all required documentation, including signature pages and fingerprints, timely.

Q: Why is electronic submission of fingerprints being mandated?
A: Manually capturing and submitting fingerprints is time consuming and prone to errors. The intent is to utilize automated electronic fingerprint devices to decrease capture, submission, and processing time. By memorandum dated July 29, 2010, the Under Secretary of Defense for Intelligence issued a requirement for Department of Defense (DoD) components to transition to electronic capture and submission of fingerprint images in support of all background investigations by December 31, 2013 (e-Fingerprint memo). Additionally, this transition will support goals established by the Intelligence Reform and Terrorism Prevention Act of 2004 and the implementation of Homeland Security Presidential Directive-12.

Q: Why are there so many options to research to identify an electronic fingerprint solution?
A: There are many approved e-Fingerprint Service Providers that provide different levels and types of service, including live scan locations and fingerprint card conversion services, to meet the needs of a variety of companies. However, not every service provider will have an option that works for every company. Additional options, including purchasing certified scanning equipment or working with other cleared companies, GCAs, or local law enforcement agencies, are available. However, each facility should determine if these options will work for their personnel. Although facilities can obtain a SWFT account for Fingerprint Submission once they are cleared, they will still need to identify an electronic Fingerprint Capture solution that meets their needs.

Q: When should we submit the electronic fingerprint file through SWFT?
A: You should submit the electronic fingerprint file to OPM via SWFT or to FCB via SAFE concurrently with signature page submission immediately after the e-QIP has been released to the DSS or no later than 14 calendar days after signature forms are submitted to FCB.

Q: Can my electronic fingerprint file be sent directly to the FBI?
A: No. It is extremely important that you confirm with the organization that will complete the Fingerprint Capture that they can transmit the electronic file to you (to be forwarded to FCB via SAFE) or to OPM via SWFT. Electronic fingerprint files that are transmitted directly to the FBI cannot be used.

Q: Do we need to provide the investigation request number on the electronic fingerprint submission?
A: It is not necessary to associate the investigation request number from the Electronic Questionnaires for Investigative Processing (e-QIP) system with the electronic fingerprint file.

Q: Once we submit the electronic fingerprint file through SWFT, when should we delete the file from our system?
A: Companies may hold the electronic file until the FBI results are posted in the Joint Personnel Adjudication System (JPAS) as a Special Agreement Check (SAC) or 120 days.

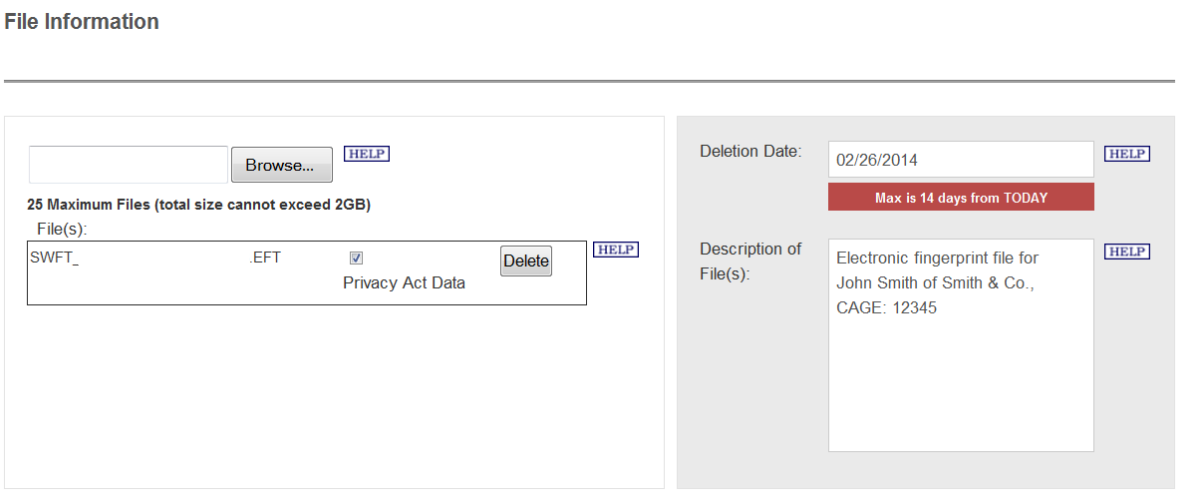
Q: I attempted to transmit a file via SAFE and now the website won't load. What should I do?
A: Verify that the file you are trying to send is not larger than 2MB. Clear your browser history and attempt to access the website and send the file again. If you continue to have difficulty, contact your FCB POC.

Appendix B: Submitting Signature Pages and Electronic Fingerprint Files to FCB

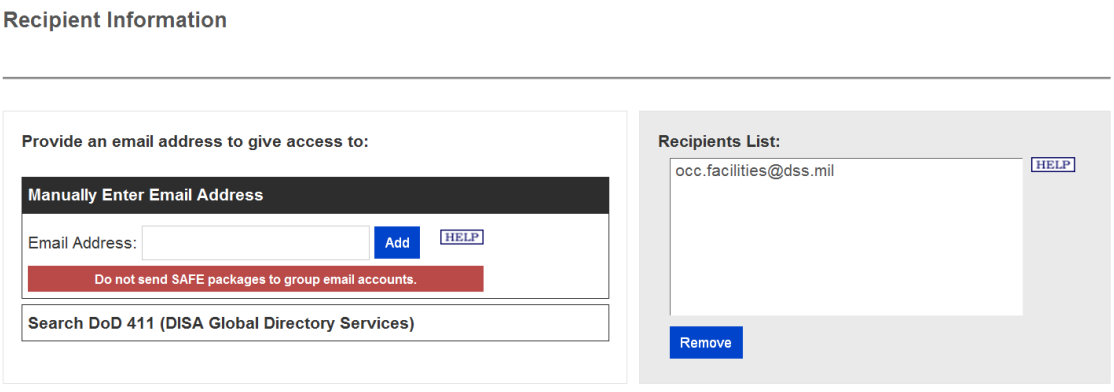
1. In your web browser, navigate to https://safe.amrdec.army.mil/SAFE/. Under Non-CAC Users, click the blue "Click Here" button.

2. In the Person Information section, enter your name and email address. *You must currently have access to this email account as you will need to verify you are the sender before the file will be sent.

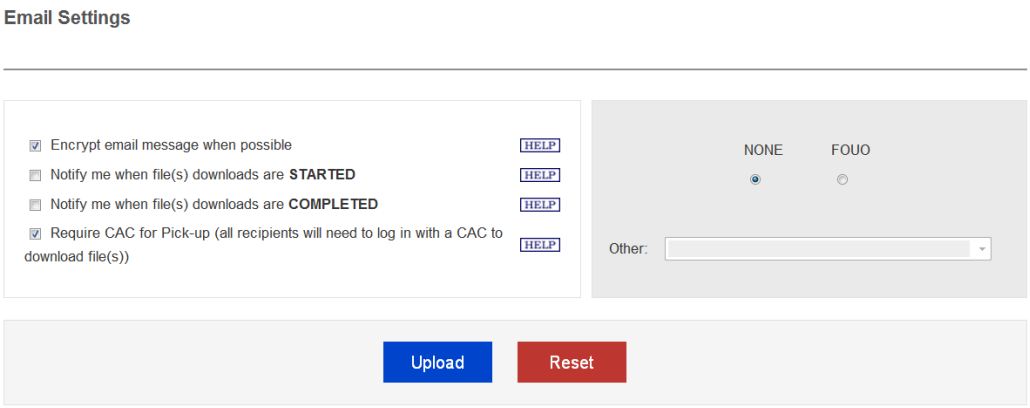
3. In the File Information section, click the "Browse…" button. Locate the electronic fingerprint .EFT or signature page .PDF file on your computer and click open. In the file list, check the "Privacy Act Data" box. The Deletion Date will default to 14 days from today. The default date is acceptable. In the Description of File(s) box, please include type of file (s) being sent (fingerprint file or signature pages or both), subject's name(s), company name, and CAGE code.



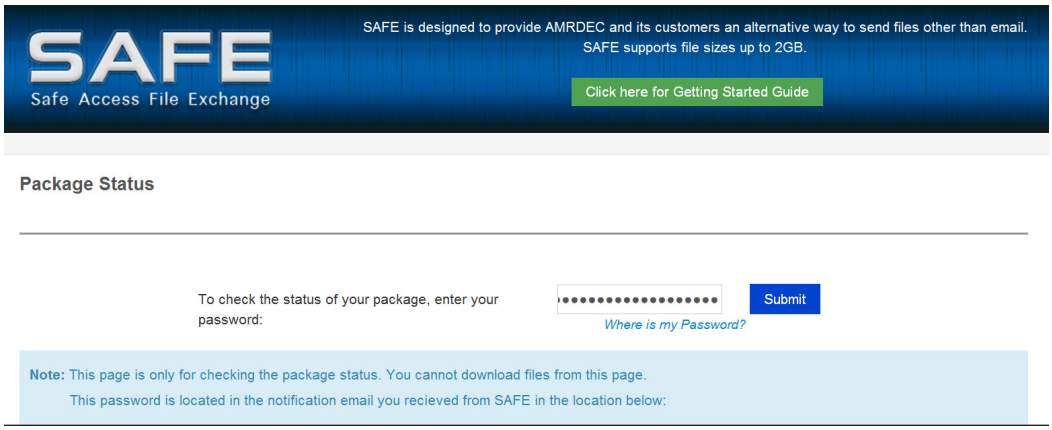
4. In the Recipient Information section, enter the email address of the FCB POC listed in your e-QIP initiation email in the Email Address box and click the Add button. You should see the email address listed in the Recipients List box. Below is an example only of the screen you should see and files should not be sent to the email address shown in the screenshot.



5. In the Email Settings section, check the "Encrypt email message when possible" box and the "Require CAC for Pick-up box." Click the blue "Upload" button at the bottom of the page. *Please note the file is not available to FCB and we will not be notified it has been sent until you complete the next steps to verify you are the sender.



6. Check your email for a message from SAFE.Team. If you do not receive the email within a few minutes, check your SPAM messages. The email will contain a link to your package following a statement that you must login and verify that you are the sender of the package. Clicking on the link will open a browser window that requests your password. The password is also contained in the email toward the bottom of the message. Enter your password and click the blue "Submit" button.



7. Verify that you are the sender of the message. A notification will be displayed indicating the file has been sent.

8. Email your FCB POC that a file has been sent so they can ensure the file is received.

Appendix C: References

- USD(I) memo, DoD Transition to Electronic Fingerprint Capture and Submission in Support of Background Investigations, dated July 29, 2010: https://www.dmdc.osd.mil/psawebdocs/docRequest/filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=DoD+memo_e-fingerprints_2010.pdf

- DMDC Personnel Security Assurance Home Page: https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=PSA
    - DMDC SWFT: https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT
    - DMDC JPAS: https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS

- DMDC Approved Service Providers List: https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=SWFT_Vendor+List.pdf

- FBI IAFIS Certified Products List: https://www.fbibiospecs.org/IAFIS/Default.aspx

- AMRDEC Safe Access File Exchange web application: https://safe.amrdec.army.mil/SAFE/