Defense Security Service

Electronic Fingerprint Capture Options for Industry

Version 3.0
August 2013

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

Table of Contents

1.0 Introduction **3**
2.0 Purpose **3**
3.0 Deployment Options **3**
3.1 Option 1: Company Purchases Equipment 4
3.2 Option 2: Companies Sharing Resources 4
3.3 Option 3: Company(s) Offering Service 5
3.4 Option 4: Third Party Vendor Provides Electronic Fingerprint File 5
3.5 Option 5: Other Government Entities 6
4.0 Implementation Plan **6**
5.0 Handling Personally Identifiable Information **6**
6.0 Funding **7**
7.0 Technical Support **7**
Appendix A **8**
Appendix B **11**
Appendix C **12**

1.0 Introduction

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). In an effort to comply with this mandate the Defense Security Service (DSS) is providing guidance to assist companies participating in the National Industrial Security Program (NISP) to transition to electronic fingerprinting. 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.

2.0 Purpose

The purpose of this document is to outline the options available for cleared companies listed in the Industrial Security Facilities Database to submit electronic fingerprint files to the Defense Manpower Data Center (DMDC) for National Industrial Security Program (NISP) applicants. DMDC provides the Secure Web Fingerprint Transmission (SWFT) system enabling industry users to upload electronic fingerprints and demographic information for applicants requiring a background investigation for a personnel security clearance. The Office of Personnel Management (OPM) receives the hardcopy fingerprints and scans the fingerprints to an Electronic Fingerprint Transmission Specification (EFTS) file to forward to the Federal Bureau of Investigation (FBI). Paper-based capture, submission and processing of fingerprints are prone to errors and are time consuming as they are mailed to OPM. 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.

3.0 Deployment Options

The following options offer alternatives for Industry to submit fingerprints electronically to initiate the background investigation. Industry may implement one or more options based on funding, mission needs and geographic locations. Companies may acquire electronic fingerprint capture/hardcopy scan devices or leverage fingerprint service providers. All fingerprint capture/hardcopy scanners must be FBI certified in order to generate compliant electronic fingerprint records. The FBI-certified product list is located on the following website: FBI-Product List. Procedures on how to register for SWFT are located on the DMDC website, under Personnel Security/Assurance, SWFT: DMDC-SWFT Homepage. The fingerprint service provider must be vetted through the SWFT/OPM registration process prior to the submission of a subject's prints.

3.1 Option 1: Company Purchases Equipment

This option allows companies to purchase electronic fingerprint capture/hardcopy scanners in order to submit fingerprints electronically to SWFT. Industry companies may purchase equipment and software using the FBI-certified product located on the following website: FBI-Product List.

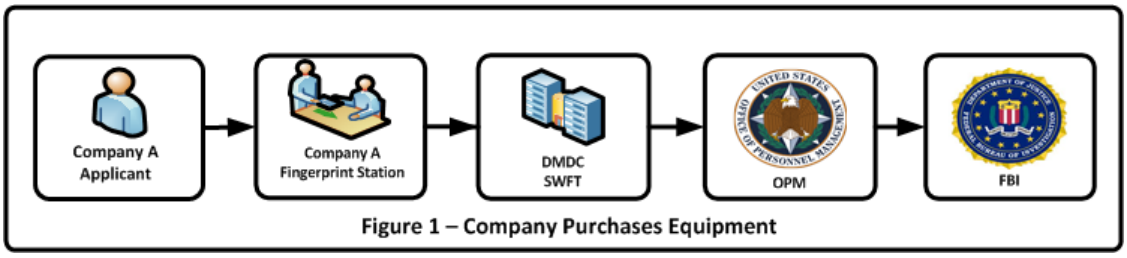

Figure 1 – Company Purchases Equipment

3.2 Option 2: Companies Sharing Resources

This option allows multiple companies to share the cost of purchasing electronic fingerprint capture/hardcopy scan devices. Beyond the initial costs, this option may require a recurring maintenance fee for sustainment. If Company A is submitting on behalf of Company B, Figure 2 shows that the owning/servicing Facility Security Officer (FSO) does not have to be involved in the actual submission of the fingerprints to SWFT.

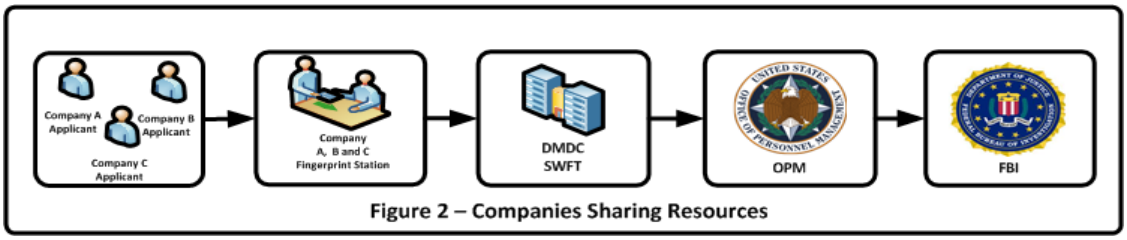

Figure 2 – Companies Sharing Resources

If companies are sharing resources but submitting their own electronic fingerprints then the equipment and software should support multiple pre-configured Company profiles. In Figure 2a the electronic fingerprint file is provided back to the FSO who will submit the file to SWFT.

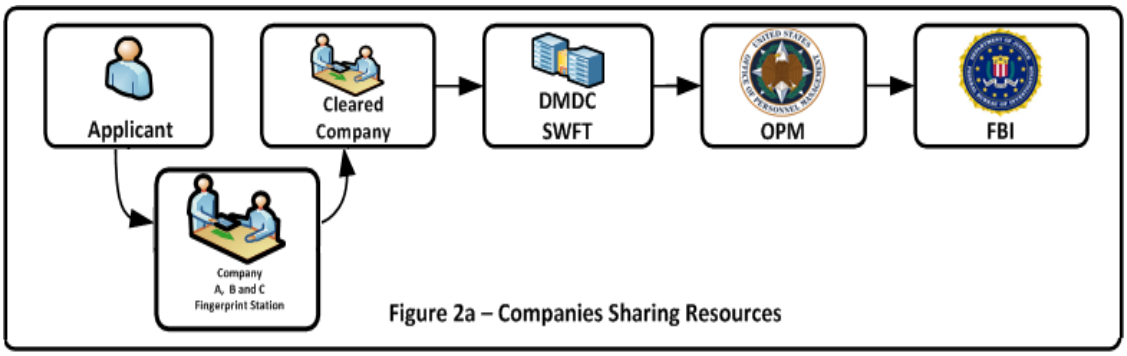

Figure 2a – Companies Sharing Resources

3.3 Option 3: Company(s) Offering Service

This option allows a cleared company to support other companies in submitting electronic fingerprints to SWFT. Companies providing the service to upload fingerprints to SWFT may submit all fingerprint files under their own CAGE Code. However, the following alternatives are available:

Full Privileges on Behalf of Another Company
Cleared companies uploading to SWFT on behalf of another company must submit a separate System Access Request (SAR) to associate the company's CAGE Code to the service provider's SWFT account.

Limited Privileges on Behalf of Another Company
Any SWFT account holder can act as a service provider for one or more companies if a "Multiple-Company Uploader" role is indicated on the SAR. This allows the service provider to submit electronic fingerprints for another company, but will not permit access to detailed SWFT reports and PII data for any of the serviced companies. Serviced companies must obtain their own SWFT account before the service provider can submit electronic fingerprints.

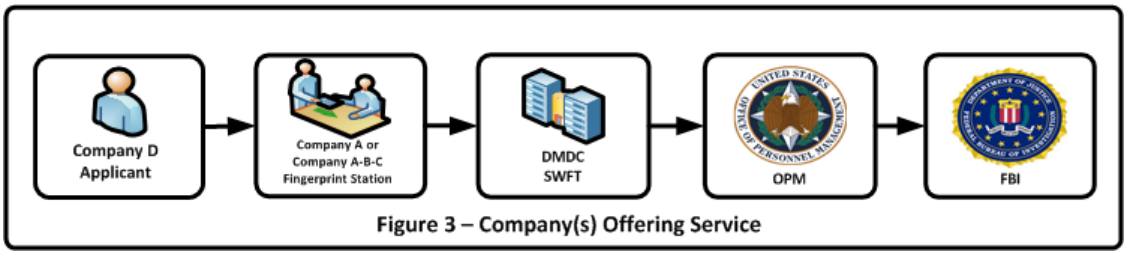

Figure 3 – Company(s) Offering Service

3.4 Option 4: Third Party Vendor Provides Electronic Fingerprint File

This option allows a company to receive the electronic fingerprint file from a third party vendor that is an FBI approved channeler. The third party vendor collects the fingerprints and saves the file in the required format to meet SWFT, OPM and FBI standards. The vendor provides the electronic fingerprint file to

the company using agreed upon file transfer methods. The owning/servicing FSO uploads the file to SWFT. The third party vendor must coordinate through the sponsoring FSO to register their equipment with SWFT prior to processing any NISP applicants.

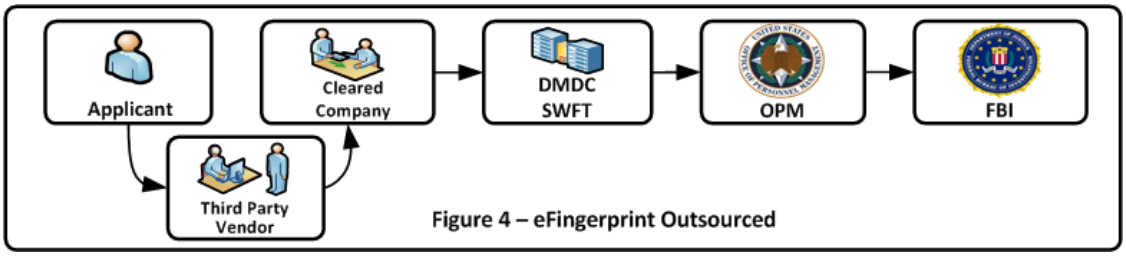

Figure 4 – eFingerprint Outsourced

3.5 Option 5: Other Government Entities

This option allows Industry to partner with the military services and other government agencies participating in the NISP (see Appendix C) for electronic fingerprint submissions. Military services and government agencies may leverage their electronic processes to submit directly to OPM. Agencies capturing Industry contractor fingerprints under the NISP must use the DSS Submitting Office Number (SON), Security Office Identifier (SOI) and the Intra-Governmental Payment and Collection (IPAC) to submit electronic fingerprints through a government entity. OPM will match the fingerprint results to the SF86 submission to initiate the investigation by using the individual's social security number.

4.0 Implementation Plan

Companies may employ multiple options depending on how widespread their cleared population is, as well as other factors that may apply to their organization. A SWFT account may be necessary and FSOs should review the SWFT Access, Registration, and Testing Procedures document to obtain information on gaining access to SWFT and registering equipment, if required. Since Option 5 allows fingerprints to be electronically submitted directly from a government agency to OPM, SWFT will not track these submissions.

5.0 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. In order to support authorized PII data sharing, DSS recommends the following:

1. Companies/vendors that wish to provide fingerprint services to other companies enter into a service agreement with each other, allowing the service provider to have their SWFT account associated with the other company's CAGE Code.
2. In the absence of a service agreement, each request for adding a CAGE Code to an existing SWFT account will require a separate System Access Request (SAR) validated by the corporate official or KMP of the company that is seeking the fingerprint services from the provider.

6.0 Funding

SWFT is a fully operational system that is funded, managed and operated by DMDC. The major funding issue for cleared contractors implementing electronic fingerprinting is the total cost of ownership of hardware that is needed to produce the electronic fingerprints. It is recommended that the company evaluate acquisition and operating costs when determining which options best suit the company's organizational needs. It is also likely that companies will seek to add any costs associated with new Government-imposed security requirements to their contract prices as an equitable adjustment.

7.0 Technical Support

The DMDC SWFT team provides support for registering equipment, coordinating test activities, and assisting with data discrepancy resolution. All other SWFT inquiries should be routed through the DMDC Contact Center or telephone (800)467-5526. The SWFT Support Team does not provide technical assistance for hardware devices; the equipment supplier or hardware manufacturer must provide this type of support.

A SWFT configuration guide is available to registered users once they access the SWFT system and download it from the Help menu.

Appendix A

Frequently Asked Questions

QUESTIONS AND ANSWERS: The following questions and answers are in response to queries or anticipated queries regarding the requirement to transition to electronic fingerprint submission for personnel security investigations:

Q: Why is this change (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. 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: How can a cleared company know what specific equipment to purchase?

A: The 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 FBI Criminal Justice Information Services Division Biometric Services Section, as part of Biometric Center of Excellence, certifies these products.

Q: What is SWFT?

A: The Secure Web Fingerprint Transmission (SWFT) program enables cleared Defense industry users to submit electronic fingerprints (e-fingerprints) and demographic information for applicants who require an investigation by the Office of Personnel Management (OPM) for a personnel security clearance. Cleared contractors collect and securely transmit e-fingerprints to SWFT for subsequent release to OPM based on a JPAS/e-QIP submission approved by the Personnel Security Management Office for Industry (PSMO-I). Paper-based capture, submission and processing of fingerprints was time consuming and prone to errors. The SWFT eliminates the manual paper process, expedites the clearance process, and provides end-to-end accountability for PII data.

Q: Why use SWFT?

A: OPM is the personnel security investigative service provider for DoD and channels the fingerprints to the FBI in order to receive the results from the record and name checks in conjunction with background investigations. SWFT was developed to provide Industry with a streamlined process and traceability of electronic fingerprint submissions.

Q: How soon can cleared facilities transition to submitting electronic fingerprints to SWFT method?

A: Any cleared facility can begin the transition to SWFT immediately using any of the options listed in Section 3.0. SWFT is a fully operational system that is funded, managed and operated by Defense Manpower Data Center (DMDC).

Q: When should we submit the electronic fingerprint file through SWFT?

A: It is recommended that the electronic fingerprint file be submitted through SWFT immediately after the e-QIP has been released to the PSMO-I.

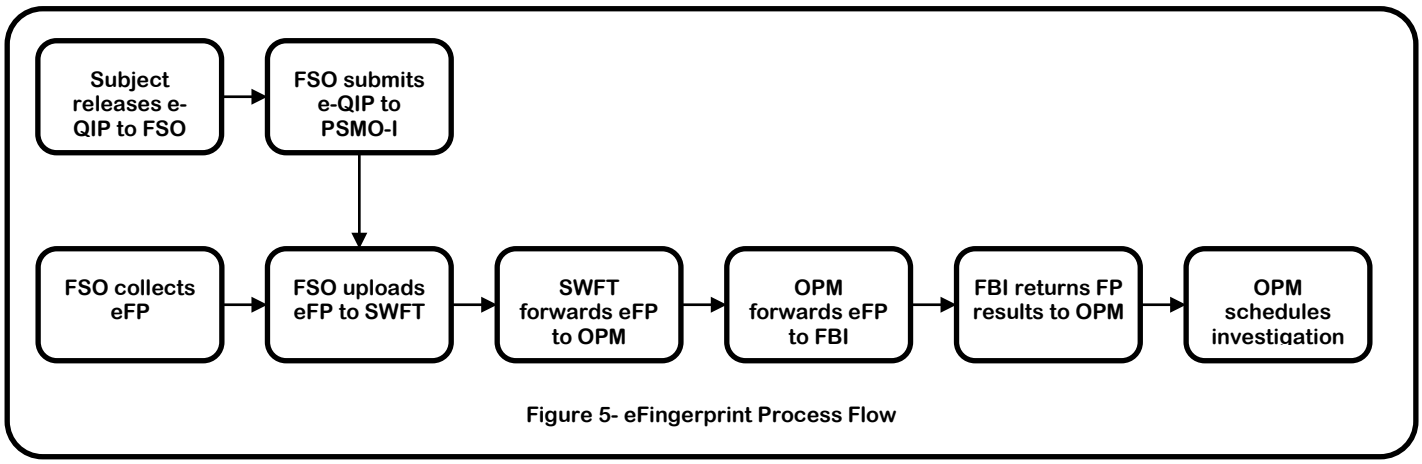

Figure 5- eFingerprint Process Flow

Q: Do we need to provide the e-QIP number on the electronic fingerprint submission?

A: It is not necessary to associate the e-QIP number with the electronic fingerprint file. In fact, there is no field to enter that data.

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 JPAS as special agreement check (SAC) or 120 days.

Q: Does a cleared facility need to own and operate fingerprint scanning devices in order to be able to use SWFT?

A: Owning or operating scanning devices is not necessary. Any cleared facility can obtain SWFT account.

Q: What are the challenges?

A: The USD-I memorandum dated July 29, 2010 mandates that fingerprints must be submitted electronically for all background investigations by December 2013. Resource issues could delay deployment, which could include availability of equipment, registration processing, machine testing, and user training.

Q: Our company has been assigned over 10 different CAGE codes, but has only two central processing stations in separate locations. Which option is optimal for our company, and how will the process actually work?

A: There are two ways a central processing station can be engaged in processing and submitting e-Fingerprints to SWFT:

1. The company or each processing station can submit all of its fingerprints under a single CAGE Code. This will, however, prevent you from being able to track and report the fingerprint transactions separately for each CAGE Code if needed.
2. The optimal approach is to request the enabling of "Multiple-Company Uploader" SWFT role for your processing stations. This will allow each processing station to upload e-fingerprints for any of the ten CAGE codes and to run reports on transactions by CAGE Code. Users of each CAGE code must maintain their own SWFT account.

Q: SWFT supports multiple CAGE codes, but the vendor who supports our fingerprint scanner advised us that they have yet to integrate multiple CAGE codes in their software. How can our FSO upload e-Fingerprints for multiple CAGE codes?

A: If you are not going to submit under the "Multiple-Company Uploader" role, you can process all submissions under one CAGE code.

Q: My company is a Third Party Vendor whose fingerprint scanners are being sponsored for use with SWFT by a cleared DOD contractor. Will I have to re-register the same equipment each time we offer services to another NISP contractor?

A: Fingerprint scanning workstations or server-based scanning systems do not have to be re-registered or re-tested before being able to service other client companies. Provide your customers with the manufacturer and serial number of your scanners, your CAGE Code, or the CAGE Code of the company 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. However, any change in your system that could affect the quality or contents of electronic fingerprint files (e.g., software patches or upgrade, hardware replacement, etc.) requires the equipment's re-test.

Appendix B

References

- USD(I) memo, DoD Transition to Electronic Fingerprint Capture and Submission in Support of Background Investigations, dated July 29, 2010: e-Fingerprint memo

- Secure Web Fingerprint Transmission (SWFT) program available now:
  - Homepage: https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT
  - SWFT Program Manager Email: dmdc.swft@mail.mil
  - Registration, Access and Testing Procedures: https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=SWFT+Access+Registration+and+Testing+Procedures+v1-2.pdf
  -
- FBI Approved List:
  - FBI-Certified Products: https://www.fbibiospecs.org/IAFIS/Default.aspx

- FBI Approved Channeler List:
  - FBI Approved Channelers: http://www.fbi.gov/about-us/cjis/background-checks/list-of-fbi-approved-channelers

- DMDC Contact Center:
  - Customer Service Hours: 6:00AM – 8:00PM EST, Monday through Friday (excluding federal holidays)
  - Toll-Free Telephone: (800)467-5526
  - Website: http://www.dss.mil/about_dss/contact_dss/contact_dss.html

Appendix C

The Secretary of Defense has entered into agreements with the departments and agencies listed below for the purpose of rendering industrial security services:

1. Department of Agriculture
2. Department of Commerce
3. Department of Education
4. Department of Health and Human Services
5. Department of Homeland Security
6. Department of Justice
7. Department of Labor
8. Department of State
9. Department of Interior
10. Department of Transportation
11. Department of Treasury
12. Environmental Protection Agency
13. Federal Communications Commission
14. Federal Reserve System
15. General Services Administration
16. Government Accountability Office
17. National Aeronautics and Space Administration
18. National Archives and Records Administration
19. National Science Foundation
20. Nuclear Regulatory Commission
21. Office of Personnel Management
22. Overseas Private Investment Corporation
23. Small Business Administration
24. United States Agency for International Development
25. United States International Trade Commission
26. United States Trade Representative