Defense Security Service

Electronic Fingerprint Capture Options for Industry

Version 1.0
April 2012

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

Table of Contents

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 connection with Defense Security Service (DSS) preparations to comply with this mandate, DSS is issuing 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. The DMDC provides the Secure Web Fingerprint Transmission (SWFT) enabling industry users to submit electronic fingerprints and demographic information for applicants requiring a background investigation for a personnel security clearance. Paper-based capture, submission and processing of fingerprints are prone to errors and time consuming as they are mailed to the Office of Personnel Management (OPM). 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). The SWFT application 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 multiple solutions for Industry to acquire the necessary hardware and software to submit fingerprints electronically to SWFT. Industry may implement one or more options based on funding, mission needs and geographical locations. Companies may acquire electronic fingerprint capture devices and/or fingerprint card scan systems. Procedures on how to register for SWFT are located on the DMDC website, under Personnel Security/Assurance, SWFT: DMDC-SWFT Homepage.

3.1 Option 1: Company Purchases Equipment

This option proposes that Industry companies purchase fingerprint capture devices and/or fingerprint card scan systems in order to submit electronic fingerprints to SWFT. Industry companies may purchase equipment using the FBI-certified product list on the following website: FBI-Product List.

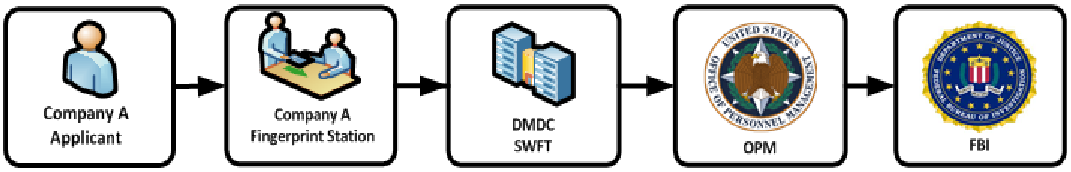

Figure 1 – Company Purchases Equipment

3.2 Option 2: Companies Sharing Resources

This option provides a solution for multiple companies to share in the cost of purchasing fingerprint scan devices. Beyond the initial costs, this option may require a recurring maintenance fee for sustainment to be paid to the entity with operational control over the solution. Equipment and software should support multiple pre-configured Company profiles. Figure 2 shows that the owning/servicing FSO does not have to be involved to submit the fingerprints to SWFT. In Figure 2a the electronic fingerprint file is provided back to the FSO to submit the file to SWFT.

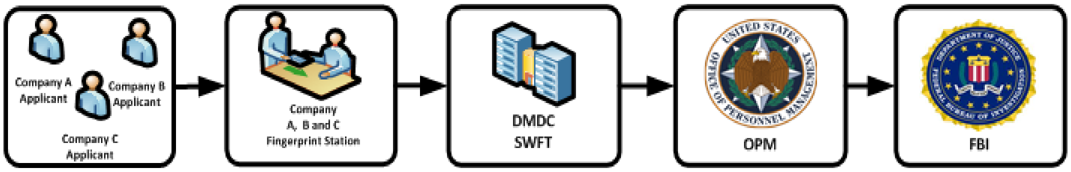

Figure 2 – Companies Sharing Resources

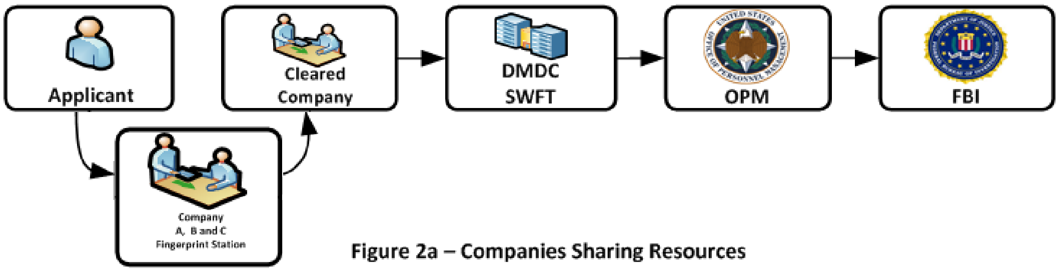

Figure 2a – Companies Sharing Resources

3.3 Option 3: Company(s) Offering Service

This option proposes that Company Purchased Equipment be offered as a service to support other companies in submitting electronic fingerprints to SWFT. This option allows smaller companies to submit electronic fingerprints without incurring the expense of purchasing and maintaining equipment. Equipment and software should support multiple pre-configured Company profiles if required by the Industry company providing the service. The configuration of multiple companies in the software configuration is not a SWFT or OPM requirement.

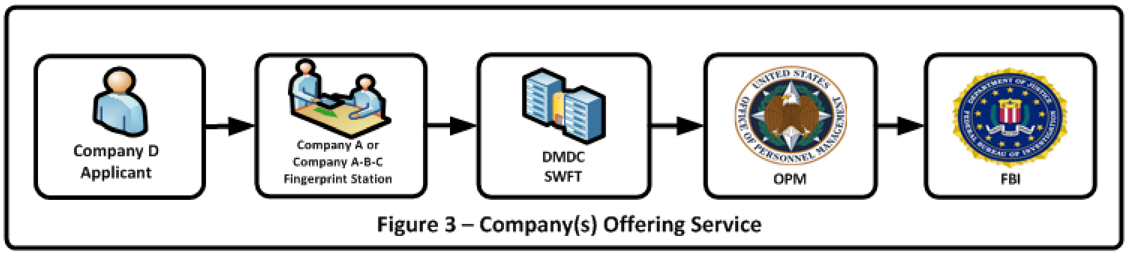

Figure 3 – Company(s) Offering Service

3.4 Option 4: Third Party Vendor Provides Electronic Fingerprint File

This solution 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 FBI standards. The vendor provides the electronic fingerprint file to the Industry company using agreed upon file transfer methods. The owing/servicing FSO uploads the file to SWFT. The third vendor must coordinate through the sponsoring FSO to register equipment with SWFT and OPM prior to processing any NISP applicants. The third party vendor may not directly forward electronic fingerprint files to OPM or SWFT.

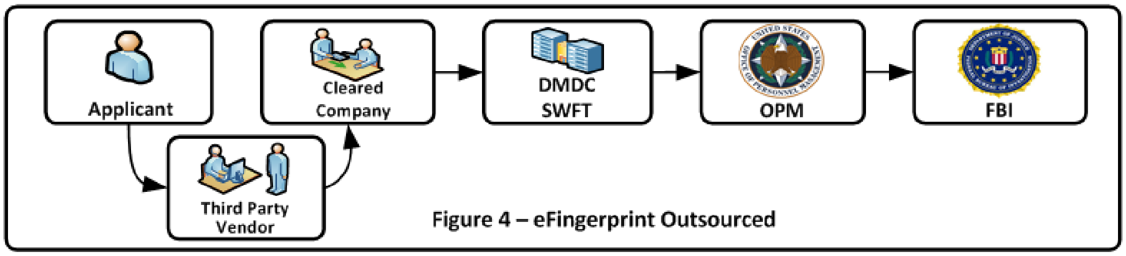

Figure 4 – eFingerprint Outsourced

3.5 Option 5: DoD Agency Support

DSS is working with other DoD agencies to provide additional solutions to meet the December 2013 electronic fingerprint submissions. This section will continue to be updated as new options are implemented and made available to NISP applicants.

4.0 Implementation Plan

Options 1 - 4

Companies may deploy multiple options depending on infrastructure and geographical locations. Companies choosing to purchase equipment and send electronic fingerprints must coordinate their registration directly with DMDC SWFT Coordinator at swft@osd.pentagon.mil. DMDC SWFT Program Manager recommends purchasing equipment prior to contacting the SWFT Coordinator. To obtain information on the Industry procedures for registering and gaining access to the SWFT system use the following website: SWFT - Registration, Access and Testing Procedures.

5.0 Funding

SWFT is a fully operational system that is funded, managed and operated by the Defense Manpower Data Center (DMDC). The major funding issue for cleared contractors implementing electronic fingerprinting is the cost for purchasing and operating the fingerprint scanning equipment and software. The purchase cost ranges from $2,000 to $20,000 per machine. The total cost incurred by the contractor for fingerprint scanning equipment will include the number of machines required to support their site(s) plus labor or ancillary items, such as maintenance.

Single User: SWFT is designed to accept fingerprints only from registered SWFT users and from registered equipment. Each user is associated with a specific CAGE Code and submission site with equipment registered with the DMDC SWFT-Program Manager and OPM Fingerprint Transmission System Program Manager. This ensures that fingerprints are received from a trusted source using approved equipment since the transmission occurs over the internet.

Multiple Users: If multiple companies are to share a machine, they will all have to reference the same registered equipment when establishing their SWFT accounts. They may also have to develop a system that will help them to keep the fingerprints separated between individual Companies and CAGE codes, and assist with industry billing.

6.0 Technical Support

It is envisioned that formal help desk support will not be required. Companies will contact the DMDC SWFT Coordinator (swft@osd.pentagon.mil) for support with the registration process, coordination of test activities, and assistance with data discrepancy resolution. All other SWFT inquiries can be routed through the DoD Security Services Center or telephone (888) 282-7682. The SWFT coordinator does not provide technical assistance for hardware devices. This type of support will come from the equipment supplier or hardware manufacturer.

A SWFT user guide located on the DMDC SWFT website is available to all registered users upon successful login to the SWFT system.

Appendix A

Frequently Asked Questions

QUESTIONS AND ANSWERS: The following questions and answers are in response to queries or anticipated queries in order to explain 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 speed 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: SWFT provides companies participating in, or applying to participate in, the National Industrial Security Program the ability to transmit fingerprint files electronically through secure web services. The process allows fingerprint images to be captured electronically, uploaded to a central collection point (SWFT server), and then released from the SWFT system to OPM and routed to the FBI. DSS has designated SWFT as the only method for submitting electronic fingerprints to OPM in association with a background investigation for NISP participants.

Q: Why use SWFT?

A: OPM is the 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 for industry to support a streamlined process and traceability of electronic fingerprint submissions. Furthermore, the Defense Security Service submits the background investigation request to OPM on behalf of Industry and incurs the cost associated with completing the investigation. Since fingerprint check results are a requirement for initial background investigation, the service fee associated with the submission is incurred by DSS as well.

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 paragraph 2.0. SWFT is a fully operational system that is funded, managed and operated by Defense Manpower Data Center (DMDC).

Q: What are the challenges?

A: The USD-I memorandum 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 how a central processing station could be engaged in processing and submission of e-Fingerprints to SWFT:

1. Company A owns one or more computer/scanner systems which have been registered with OPM and SWFT. The user account of the central processing station staff member (e.g., FSO) is not only associated with the CAGE Code of Company A, but also with CAGE Codes of the Company’s branches B, C, D, etc. Person from Company A or any of its branches comes to the central processing station, has the fingerprints scanned, and the e-Fingerprint is generated. The FSO then logs into the SWFT system and selects the CAGE Code that will be used in this session. Then the FSO uploads to SWFT all e-Fingerprints that are associated with the selected CAGE Code. The same process will be used to submit e-Fingerprints for any other CAGE Code that the FSO has been registered to use.

2. Company A owns one or more computer/scanner systems, which have been registered with OPM and SWFT. The user account of the central processing station staff member (e.g., FSO) is associated only with the CAGE Code of Company A. If the Company has multiple branches B, C, D, etc., then their FSOs establishes their own SWFT user account. Person from Company A or any of its branches comes to the central processing station, has the fingerprints scanned, and the e-Fingerprint is generated. The staff member of the appropriate Company or branch later logs into the SWFT system from any secure location (it doesn’t have to be collocated with the central processing station), and uploads the e-Fingerprint to SWFT.

Q: The SWFT supports multiple CAGE codes, but the vendor who supports our fingerprint scanner advised us that they have not yet integrated multiple CAGE codes in their software. How can our FSO upload e-Fingerprints for multiple CAGE codes?

A: SWFT system does not extract CAGE Code from e-Fingerprint files. SWFT system only registers the CAGE Codes of its users (e.g., FSOs) to support the upload of e-Fingerprint files and view reports tied to CAGE Codes. This is intended to provide security and accountability for the PII data uploaded and stored in SWFT. The process of generating the e-Fingerprint file (action taken on a fingerprint scanner), and the process of uploading the e-Fingerprint to SWFT (action taken on any computer with web browser) are two separate, asynchronous and independent processes. The FSO first scans a person's fingerprint and generates the e-Fingerprint file. This process can be repeated for multiple persons as needed. Later, the FSO logs into the SWFT system from any secure location (it does not have to be collocated with the fingerprint scanner), and uploads the e-Fingerprints to SWFT.

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: swft@osd.pentagon.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+Registration+Access+and+Testing+Procedures_1_9.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

- DoD Security Services Center:
  - Customer Service Hours: 6:00AM – 8:00PM EST, Monday through Friday (excluding federal holidays)
  - Toll-Free Telephone: (888) 282-7682
  - Website: http://www.dss.mil/about_dss/contact_dss/contact_dss.html