Defense Security Service

Electronic Fingerprint Capture Options for Industry

Version 2.0
January 2013

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 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. 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. 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 the Office of Personnel Management (OPM). 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 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 other service providers. 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. Prior to working with any service provider collecting and/or transmitting fingerprints to SWFT and OPM, please note, these vendors 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.

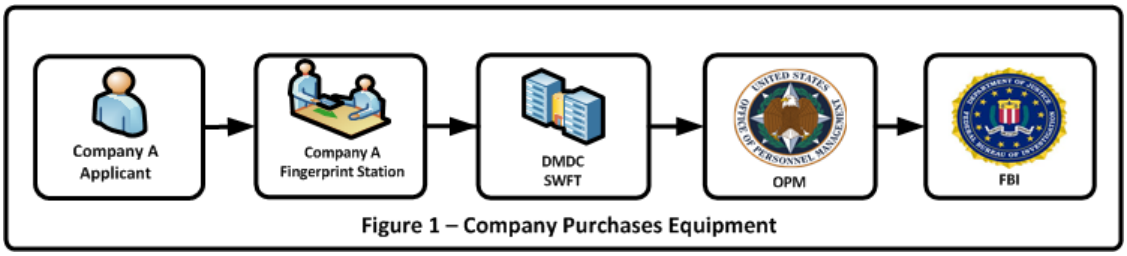

Figure 1 – Company Purchases Equipment

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.

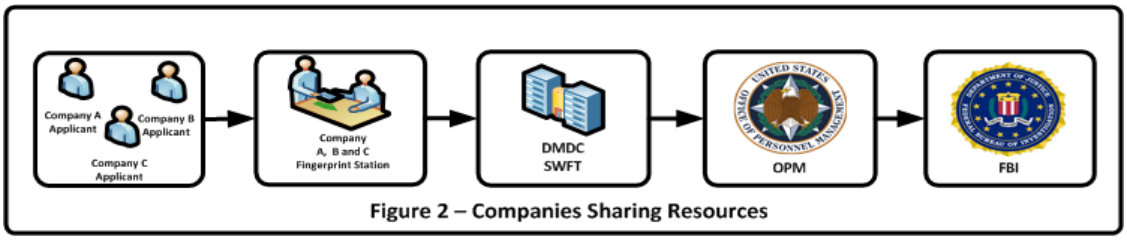

Figure 2 – Companies Sharing Resources

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.

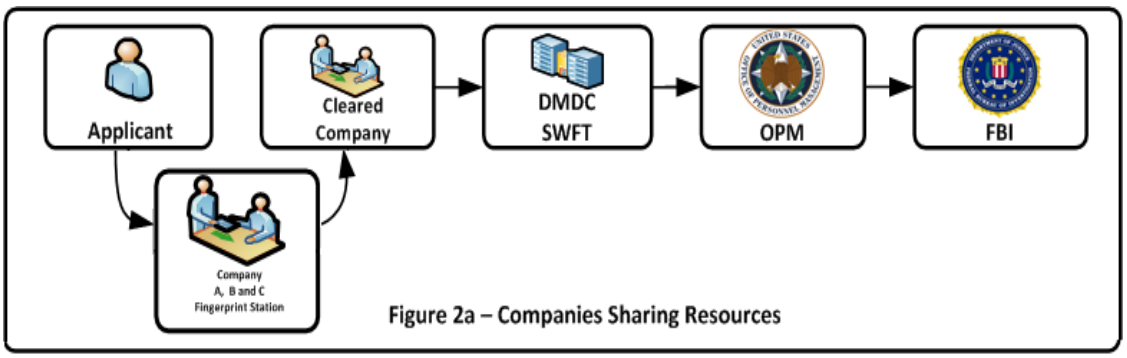

Figure 2a – Companies Sharing Resources

3.3 Option 3: Company(s) Offering Service

This option allows Company Purchased Equipment to be offered as a service to support other companies in submitting electronic fingerprints to SWFT. This option permits a cleared company to submit electronic fingerprints on behalf of other cleared companies. Cleared companies must submit a letter of authorization on company letterhead, signed by a Key Management Personnel (KMP) or corporate official authorizing another cleared company to submit electronic fingerprints on their behalf.

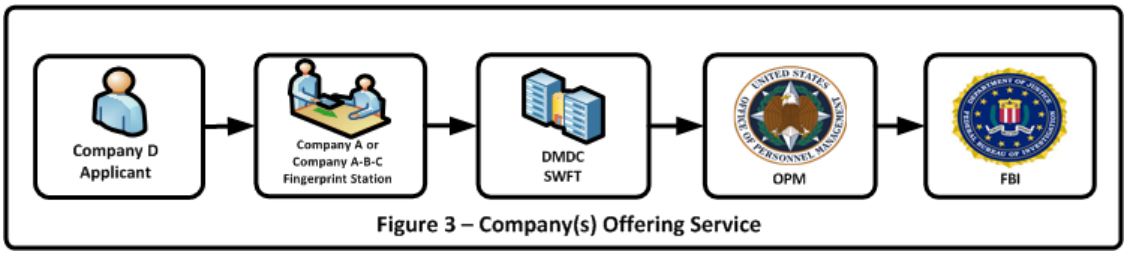

Figure 3 – Company(s) Offering Service

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. The third party vendor may submit electronic fingerprint files to SWFT on behalf of a cleared company with a letter of authorization.

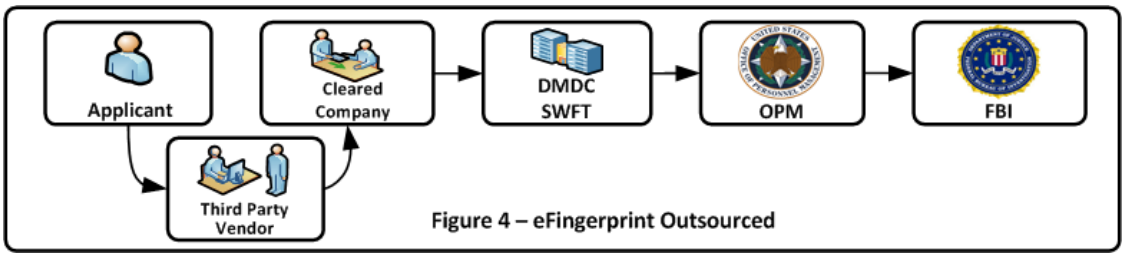

Figure 4 – eFingerprint Outsourced

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. It is not necessary to use the DSS Submitting Office Number (SON) and Security Office Identifier (SOI) to submit electronic fingerprints through a government entity. OPM will match the fingerprint results to the SF86 submission to initiate the background investigation by using the individual's social security number. The SF86 submission will incur the investigation cost to DSS which includes the FBI fingerprint check.

4.0 Implementation Plan

Companies may deploy multiple options depending on how wide spread 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 - Registration, Access 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 Personally Identifiable Information (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 who wish to provide fingerprint services to other companies enter in an agreement with each other, allowing the service provider to have their SWFT account be associated with the other company's CAGE Code. DMDC will receive a copy of any such agreement prior to associating SWFT account with CAGE Codes of other/unrelated companies.

2. In the absence of an agreement, each request for adding a CAGE Code to existing SWFT account of the service provider 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 the Defense Manpower Data Center (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.

Single User: SWFT is designed to accept fingerprints from SWFT users and registered equipment. A SWFT user may be associated with multiple CAGE Codes (e.g., Cage Codes of subsidiaries of a large company). This ensures that fingerprints are received from a trusted source using approved equipment.

Multiple Users: If multiple users share equipment, the equipment will be tested only once. The users will 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.

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 DoD Security Services Center or telephone (888) 282-7682. The SWFT Support Team does not provide technical assistance for hardware devices. This type of support will come from the equipment supplier or hardware manufacturer.

A SWFT configuration guide is available to registered users once they login into 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 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 is Secure Web Fingerprint Transmission. 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 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. Furthermore, the Defense Security Service submits the personnel security investigation request to OPM on behalf of Industry and pays for the cost associated with completing the investigation. Since fingerprint check results are a required element for all initial personnel security investigations, the service fee associated with the submission is funded 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 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 how a central processing station could be engaged in processing and submission of e-Fingerprints to SWFT:

1. Company A owns one or more electronic fingerprint capture/hardcopy scan devices, 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. Subject ((i.e., the clearance applicant) 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. A large company may choose to submit e-Fingerprints for their subsidiaries under a single CAGE Code.

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 establish their own SWFT user account. Subject 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: The 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 uploaded and stored in SWFT. The process of generating the e-Fingerprint files (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: dodhra.dodc-mb.dmdc.mbx.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+v1.1.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

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 Science Foundation
19. Nuclear Regulatory Commission
20. Office of Personnel Management
21. Small Business Administration
22. United States Agency for International Development
23. United States International Trade Commission
24. United States Trade Representative