ASKDISCO 003-12 WEBINAR

September 27, 2012

DISCO hosted its third installation of AskDISCO Webinar which covered the future of DoD CAF and provided several points of clarification on eFingerprinting and SWFT. This document contains the general questions received concerning the aforementioned topics.

AskDISCO 003-12 Points of Reference

The following links have been provided as quick points of reference to further assist you familiarizing yourself with the incumbent changes related to e-Fingerprints and the DoD CAF Consolidation as well as to provide supplemental information to the webinar that was presented on August 28, 2012.

1. Electronic Fingerprint Capture Options for Industry
2. Access & Registration-Slideshow
3. Access, Registration, Test Guide
4. Company Vetting Form
5. SAR Form
6. FBI-Product List
7. DoD Transition to Electronic Fingerprint Capture and Submission in Support of Background Investigations

AskDISCO 003-12 Questions & Answers

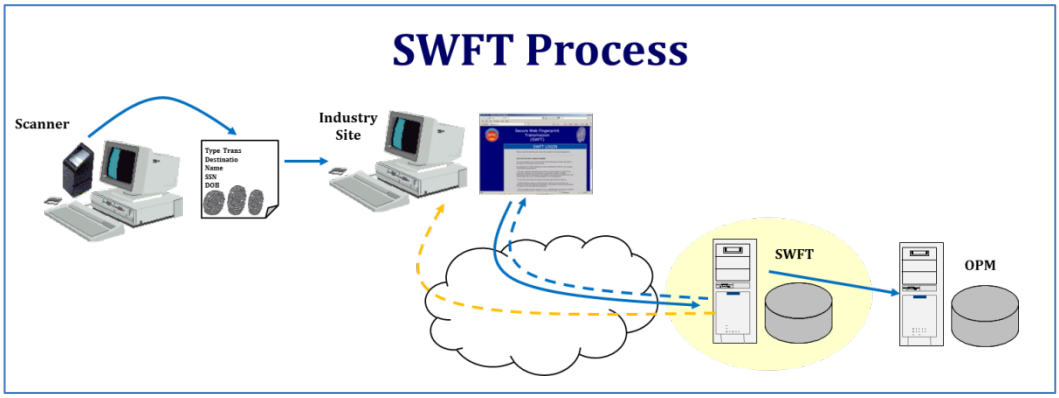
e-Fingerprinting

SWFT REGISTRATION & PROCESS

1. Where do you apply for a SWFT account?
    a. Obtain the System Access Request (SAR) form from the SWFT website https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT . Submit the completed SAR to the DoD Security Services Call Center (see details on the SWFT website).

2. Should we obtain a SWFT account prior to acquiring hardware?
    a. It is an acceptable practice to sign up for your SWFT account prior to acquiring hardware.

3. When I transmit fingerprints through the SWFT system where do they go? In other words, what is the work flow?
    a. SWFT is a Store and Forward application. Electronic fingerprints are stored temporarily in SWFT until they are forwarded to OPM and then to FBI who processes the fingerprints and returns the results back to OPM within 3 business days. The final destination of those electronic fingerprints is OPM whereby the EFT file will be incorporated into the background investigation.



4. I rarely ever have to submit fingerprints, so when should I register in SWFT? I would hate to wait until I actually need it, but don't know how to ensure it works in the meantime.
    a. You can request a SWFT account at any time. However, after obtaining the account, you will have to log into the SWFT at least once every 60 days to prevent deactivation of your account. Access to the SWFT system also provides access to online User Guide, Scanner Registration Guide, and other information and guidance that will become useful when processing e-fingerprints.

5. How soon can I begin transmitting fingerprints once I've purchased and registered my equipment?
    a. Once you've purchased and completed online registration of your equipment, contact your SWFT coordinator and indicate that you are ready to schedule a test. Your SWFT coordinator will set a date for a test submission e-fingerprints (EFT files) through SWFT to OPM to ensure that your equipment is properly configured and that your e-fingerprint files comply with all standard requirements. The time frame from date of purchasing the scanner to "going live" with fingerprint submissions could range from 10-30 days.

6. If we go buy a SWFT system, we can't do any fingerprints unless FBI provides our company a UNIQUE TCN number. Correct? How do we get that?
    a. The TCN number consists of two parts: the TCN prefix (refer to the SWFT Configuration Guide* how to quickly and easily construct a prefix that will be unique for each of your scanners), and the TCN suffix that is automatically generated by the scanner (refer to your scanner documentation). FBI is not involved in this process.

7. How long does it take to get FBI approval of a SWFT application? Is there a way to get updates on the status?
    a. FBI is not involved in the approval process. The SWFT user account is approved by the DMDC SWFT, and the registration of scanning devices is done jointly by the DMDC SWFT and OPM. The entire approval process can take less than 30 days if the SWFT applicant is fully engaged in the application and registration process. The status of the registration process is available online (requires SWFT account).

8. Will we know immediately if the prints are good enough for the FBI?
    a. FBI is not involved in the SWFT approval, registration, and test process. Production tests of the scanning devices are done jointly by the DMDC SWFT and OPM. Results are generally available within 24-48 hours after the test EFT files have been submitted to SWFT. Typically, a good quality scanner software performs real-time check of the quality of each fingerprint before allowing the operator to finalize the e-fingerprint file.

9. When applying for a SWFT account, if Option 3 is used, should the FSO be listed on the SAR as the Industry Site Administrator or Industry User?.
    a. Option 3: Companies offering SWFT services to colleague companies have two options: (1) The Company that is offering the service will scan the fingerprints and generate the e-fingerprint for a Subject from the colleague company, and afterwards provides the EFT file to the company. The receiving company can have their own SWFT account and upload the EFT to SWFT by themselves. In this case, the FSO of the Company that is offering the service is not involved in account management of the colleague company. (2) The Company that is offering the service will scan the fingerprints, generate the e-fingerprint for a Subject

from the colleague company, and then uploads the EFT file to SWFT. In this case, the FSO of the Company that is offering the service also needs a SWFT user account that is associated with the Cage Code of the colleague company. The SAR for such an account must be validated by appropriate approving authority from the receiving company, as well.

10. Does each individual in the security office need a SWFT account or do we get one account for the whole office?
    a. Each SWFT user must obtain a separate user ID and password. Sharing user account information is a violation of SWFT security policy and will result in suspension of the SWFT user privileges. It may also impact the security clearance of the offender.

11. In my corporation we have 3 cage codes for separate subsidiaries. Do we need to have 3 separate SWFT accounts?
    a. If the parent company determines that handling all its subsidiaries' fingerprints through a single FSO does not pose any privacy issues, then that FSO has a choice: they may either submit the EFTs under a single Cage Code, or submit them under the Cage Codes of the individual subsidiaries.

AVAILABLILITY/SHARING

12. If a company shares SWFT equipment with another company, are there any potential liability issues associated with having PII on the colleague company's personnel stored in your SWFT?
    a. If the companies agree to share equipment the liability issue is also a shared responsibility.

13. Besides DoD agencies, is it possible to reach agreements with other agencies such as the VA to support SWFT?
    a. DSS is working with other DoD entities to provide additional solutions to meet the December 2013 electronic fingerprint submissions. It is permissible for Industry to partner with the military service community and other agencies that participate in the NISP (see Appendix C) to submit fingerprints electronically. In order to ensure that the fingerprints results are associated with the correct background investigation, the government entity must have the capability to identify Defense Security Service's SOI and SON information in the appropriate fields of the electronic fingerprint submission.

14. Will DoD be deploying eFP machines that are SWFT compatible in battlefield areas for PRs?
    a. For initial investigations, there are some DoD installations submitting to OPM and not registered to submit through SWFT. This is a viable option as long as the installation can support the requirement of Industry's SON/SOI. To be clear, there is no policy requirement to submit fingerprints for PRs.

15. My company usually hires individuals from various locations throughout the country and has fingerprints taken at local police departments; will there be any facilities other than military and cleared facilities that will be available for taking fingerprints with SWFT?
    a. You are permitted to utilize the resources at your local law enforcement facility, however, you must ensure that the equipment is registered with SWFT. If the law enforcement agency **is not** registered in SWFT then the transmission to OPM will be unsuccessful. Therefore, you may be forced to obtain the hard copy fingerprint card from local law enforcement and you will then need to use a **registered** card scanner to upload into SWFT. Ultimately, the card scanning equipment needs to be registered with SWFT for proper routing and billing as it relates to the effective processing of the electronic fingerprints.

16. Can military recruiting stations be used as 3rd party e-fingerprint stations? Also please confirm the date that hard copy fingerprints will no longer be accepted.
    a. DoD is currently evaluating all options for use of other DoD resources.

OPTIONS

17. Can a company that purchases the SWFT equipment decide to offer services outside its other organizations and charge a service fee or can the SWFT equipment only be used within your company as generating revenue can help pay for the equipment?
    a. Please refer to the Electronic Fingerprint Capture Options for Industry guide for information regarding Option 3. Once the equipment has been registered and tested with the SWFT and OPM, it can also be used for fingerprinting personnel from other companies. These other companies don't have to re-register the equipment that is used to fingerprint their employees.

18. Does the SWFT option replace submitting fingerprints through the mail? When does this start?
    a. Yes. It can start as soon as you have a SWFT account and have registered and tested your e-finger print device. All fingerprints must be electronic by December, 2013.

19. Do we need a SWFT account if we are using options 1, 2, or 3?
    a. For options 1 and 2, a SWFT account is required. For option 3, a SWFT account is not required if the company submits fingerprints electronically on your behalf.
    b. Use of the SWFT is not mandatory. If you are already submitting electronic fingerprints via some other mechanism, then you do not need to convert to SWFT. However, if you are currently unable to submit electronic fingerprints, then, depending on the option you choose, you might need to obtain a SWFT account. Please see Points of Reference above.

20. If we plan to use a 3rd party vendor to process fingerprints, do we still need to set up a SWFT account?
    a. Having your own SWFT account will enable you to receive e-fingerprint files from the 3rd party vendor, and then upload them to SWFT under your own account and Cage Code. This will also mitigate any potential Privacy Act issues.

21. What is the threshold (number of FP's submitted per year) that determines if/when a company is required to purchase their own equipment?
    a. There is no such threshold. Whether and when the company determines to procure its own scanning equipment depends entirely on the company's own cost/benefit analysis.

22. What is the difference between third party vendor and fee for service option?
    a. Fee for service option: cleared company to provide electronic fingerprint capture service
    b. 3rd party vendor: outside of the NISP, for example, FBI Channeler

23. What advantage is provided through electronic fingerprinting?
    a. There are several advantages.
        i. OPM begins investigations faster
        ii. Once you submit the e-fingerprints, you have 120 days to submit the e-QIP to DSS
        iii. Eliminates cost and time associated with mailing hardcopy fingerprints to OPM

24. I am a contractor who will have to submit fingerprints for a Government customer who needs them to process a NACLC. How will I submit from my terminal and be able to show it is for them?
    a. The SWFT system provides online reports that are exportable and printable.

PII

25. If our employee, in another state, goes to a vendor in that state, is it safe for the vendor to email the file to our office so we can upload it to SWFT?
    a. Yes, the vendor can simply capture the fingerprints, and send your FSO an encrypted email containing them.. This mitigates the PII concern.

26. What is the minimum amount of PII that is necessary for an eFP record to be accepted by SWFT? (e.g. from a visiting contractor)
    a. Full name, date of birth, place of birth, citizenship, SSN, race, and gender. There are several other data items (e.g., height, weight, eye color, hair color, etc.) that are mandated by the OPM and FBI.

27. Will there be guidelines regarding the protection of PII information?
    a. There are currently no posted guidelines regarding PII data protection that would apply specifically to SWFT. To mitigate any potential Privacy Act issues, small companies are encouraged to use a 3rd party vendor to only capture the electronic fingerprints and save the EFT file in an encrypted form, and then upload the EFT file to SWFT under their own SWFT account and Cage Code. DMDC and the SWFT team continue working on providing additional guidelines and alternatives.

TECHNICAL

28. I've read where 4-finger printing is required for DoD Industry clearances, but there are many items on the FD-258 item approved hardware list that handle only 1 or 2 fingers. So are 4-finger prints required?
    a. Everything that is required on the FD-258 hardcopy is required in the electronic fingerprint submission.

29. Should we maintain any digital backups of fingerprints until we are sure that they are accepted? How will we know when the acceptance is good?
    a. You may feel free to keep a backup copy of the EFT file but you do not have to. You can check the life cycle of the fingerprint via SWFT's online Discrepancy Report that details when the fingerprint was uploaded to SWFT, when the EFT file left SWFT and was transmitted and accepted to OPM.

30. And if we keep that back up copy, we can use that if someone goes from Secret to Top Secret? No more than one time fingerprinting....Correct?
    a. DSS does not have any recommendations regarding this subject.

SWFT EQUIPMENT

31. Does SWFT equipment have to be on a dedicated system or can it be attached to someone else's workstation?
    a. This is based on vendor configuration. You may opt to use a separate vendor for hardware versus software so ensure that you are clear on the functionality prior to moving forward.
32. Has there been any testing of the SWFT software in a virtual environment?
    a. The SWFT is a web-based system that requires no software components to be installed on the client's computer other than the internet browser. Virtual environment is part of the SWFT infrastructure support, which is transparent to the end users.

LIMITATIONS

33. Where can we find a list of approved fingerprinting facilities or companies with the proper equipment that we could utilize for option three?
    a. DSS does not maintain a list, nor are we be able to supply one. Please reach out to your contacts within your security community for this information.

34. I have heard that some companies charge a per fingerprint fee atop of the fingerprint service fee for use of their software as well as requiring the company to buy the software license. Is this true?
    a. Due to ethical limitations, we are unable to comment. Please reach out to your contacts within your security community for this information.

35. If we send specs to DSS, can you tell us if a particular reader is approved?
    a. Due to ethical limitations, we cannot make any recommendations for one vendor or another. Please reach out to your contacts within your security community for this information.

36. Does the DSS offer or plan to offer a site dedicated to letting companies know sites with in their area that offer these services to help companies that do not have SWFT equipment or accounts?
    a. Due to ethical limitations, DSS does not maintain a list of service providers. Please reach out to your contacts within your security community for this information.

GENERAL e-FP

37. When can we apply for a TCN number?
    a. When you apply for your SWFT account, your SWFT Coordinator will help you set up your Transaction Control Number (TCN).

38. Are our DSS reps going to be briefed on all of this so they know what is going on?
    a. DSS Reps are continuously briefed on all personnel security processes.

39. We can purchase a scanner to scan the prints off a hardcopy fingerprint card but the paper fingerprint card is going away. Correct? Did I miss an important part of this puzzle?
    a. Hardcopy fingerprint card can be scanned by a special scanning device and converted into an electronic fingerprint file, which can be electronically submitted through SWFT. The card scanning device, like the fingerprint scanning device, has to be registered and tested with the SWFT and OPM.
    b. For more information, please see DoD Transition to Electronic Fingerprint Capture and Submission in Support of Background Investigations.
    c. It is recommended that you search online for hardcopy fingerprint forms for purchase if your plan is to use a hardcopy scanner.

40. We plan to continue using hard copies and have the vendor scan the fingerprints. Will we still be able to get the hardcopy fingerprint cards in the future?
    a. Please see DoD Transition to Electronic Fingerprint Capture and Submission in Support of Background Investigations.
    b. Recommend searching online for hardcopy fingerprint forms for purchase if your plan is to use a hardcopy scanner.

41. What happens if FBI rejects the fingerprints?
    a. You will be required to resubmit a new set of fingerprints if rejected by the FBI.

42. What is an FBI Channeler?
    a. Please see http://www.fbi.gov/about-us/cjis/background-checks/fbi-approved-channelers.

43. Do we still have 14 days to upload the fingerprint card via SWFT after the PSQ has been sent in JPAS or will the timeframe be shortened since we will only be able to upload to SWFT?
    a. Yes, however, DSS does not recommend you wait that long once you have released the PSQ in JPAS.

CAF Consolidation

44. If more information is needed prior to Adjudication, will an Eyes Only package be received by DoD CAF or will it still go to DOHA?
    a. It will be sent to DoD CAF and be routed internally.

45. Will the consolidation of DOHA into the new DoD CAF increase the timeliness of processing cases lingering in DOHA for more than a year?
    a. Yes. A streamlined organization with adequate resources and manpower to process cases more quickly should help to alleviate this scenario.

46. Is there anything you can share WRT a plan for telephone operators manning the call center?
    a. There are no planned changes with respect to the DoD Security Services Call Center.

47. With one DoD CAF, how will this affect Loss of Jurisdiction from another CAF?
    a. This issue is scheduled to be addressed NLT 18 Nov 2012.

48. What about if the SCI CAF loads an LOJ and collateral is still in place how is that going to affect the clearance?
    a. This issue is scheduled to be addressed NLT 18 Nov 2012.

49. Should we put DISCO in the beginning of the incident when we submit to DOD CAF?
    a. No, this is not required.

50. When should Navy start to submit RRU's and incident reports to DoD CAF?
    a. The projected date for the Navy is 27 Jan 2013.

51. Will the adjudication/granting of eligibility now be posted in JPAS for all the CAFs consolidated into DoD CAF?
    a. The notation of a grant/denial for any clearance will now say DoD CAF. All messages coming from JPAS to you will say DoD CAF.

52. For SCI submittals that previously went to the AFCAF, etc, will they begin to be adjudicated by the DoD CAF as soon as the AFCAF joins the DoD CAF?
    a. Yes.

53. If DOHA is consolidated into the DoD CAF, how will we be notified that investigations are being forwarded for further investigation or appeals?
    a. The same notification process will be used until further notice.

54. When are we going to get suitability adjudications performed at CCF?
    a. This process is projected to start FY14.

General Questions

55. Having issues viewing PowerPoint, is there a download for this?
    a. Yes. The PowerPoint and audio will be posted to the DISCO Webinars & Toolkits within one week of the live event.