AskDISCO 002-12 Webinar

August 28, 2012

DISCO hosted Webinar which covered the future of eFingerprinting and SWFT as well as SF-312s. This document contains the general questions received concerning the afore mentioned topics.

AskDISCO 002-12 Questions & Answers

SF-312, Nondisclosure Agreement

1. Does the acceptance section HAVE to be signed by the contract representative?
    a. An authorized representative of a contractor designated to act as an agent of the United States, may witness and accept an SF 312 executed by an employee of that same organization. For further guidance on the SF-312 please refer to http://www.archives.gov/isoo/training/standard-form-312.pdf
2. Does the witness also have to be an employee of yours?
    a. No, the witness can by any federal employee.
3. Can the witness and the contract rep signatures be the same person?
    a. Yes, they can be the same person as long as they are an authorized contract representative.
4. Can the FSO be both witness and acceptor?
    a. Yes, the FSO can be both the witness and acceptor.
5. I would like to verify mailing address of the SF-312?
    a. You may mail the SF-312 to the following address or fax it to 301-833-3912.

    Defense Industrial Security Clearance Office
    600 10th Street, Suite 160
    Fort Meade, MD 20755

eFingerprint/SWFT

1. Can we submit FP cards for a neighboring small company using their CAGE code?

    a. Yes, if you have an agreement between your company and the other company you may submit the fingerprints through SWFT for that company under their CAGE code. In order to submit for another company, you must have the CAGE code listed under your login within SWFT to support the process. Another option is to generate the eFP for the small company, then let them upload it to SWFT under their own SWFT account.

2. When should we expect to see the presentation on line?

    a. The presentation will be posted at http://www.dss.mil/disco/indus_disco_webinars.html

3. I3 has a service whereby we can send them the fingerprint cards; they scan them and return to FSO using PKI. Will this be acceptable to DSS?

    a. DSS does not endorse any particular company. The process that you have described falls within Option 3 of the DSS Implementation Guide and meets the intent of the guide. Note: The equipment/software used must meet SWFT guidelines and must be registered through a cleared company. Both the cleared company and the service provider must ensure PII data is protected.

4. How do I find who has an a SWFT-registered scanning station in my area?

    a. Neither, Defense Security Service (DSS) nor the Defense Manpower Defense Center (DMDC) SWFT team maintains a list of EFT machines for public distribution. You may wish to network within your local NCMS chapter to see if anyone is willing to share services.

5. Can you get regular fingerprints taken (ex. Law Enforcement agency) and purchase a Fingerprint Reader and scan them in?

a. Yes you can. Please refer to the FBI Certified Product List website for a listing of approved fingerprint card scan systems. https://www.fbibiospecs.org/IAFIS/Default.aspx

   However, many law enforcement agencies are moving toward an electronic fingerprint capture system which poses several challenges to pass the EFT to SWFT. Each machine that will be used for collecting fingerprints must be registered through the cleared company that will be using the system. Local law enforcement agencies are non-cleared agencies and cannot submit directly to SWFT or OPM, thus presenting a logistical challenge of getting the EFT file and associated PII data from the LE agency to the FSO to submit through SWFT.

6. Can we use an EFT service by a third-party vendor, who scans and sends the file to the FSO via PKI?

   a. Yes, this process would fall under Option 3 of the DSS Implementation Guidance. Note: The equipment/software used must meet SWFT guidelines and must be registered with SWFT and OPM through a cleared company. Both the cleared company and the third-party vendor must ensure PII data is protected.

7. Will local FBI offices have SWFT machines?

   a. No.

8. Does bulk upload of e-fingerprints mean you can select multiple files at once to upload, and what's the max?

   a. SWFT allows users to select multiple EFTs for placement into an upload staging area. In order to be able to utilize this bulk-upload feature, Adobe Flash Player 9.0.24 or later must be installed and enabled in your browser. Prior to installing Flash please check your company's IT policy. Free download is available at http://get.adobe.com/flashplayer/.

9. Can we start using the devices and submit production EFT files when we are ready?

   a. Once the EFT submission test has been successful and approved by the SWFT Team,

you can start using your devices to submit electronic fingerprints to SWFT.

10. If I buy a machine for my office in South Carolina, will my office in Virginia be able to use it too?
    a. Yes, as long as the device has been registered and tested.
11. How does the EFT file get associated with the e-QIP investigation request at OPM?
    a. OPM uses the applicant's SSN to link the EFT file with the e-QIP submission.
12. Should we get a SWFT account now even if we're not ready to use EFT?
    a. You can get a SWFT account now and then initiate the equipment registration when you are ready. Once you have the equipment /software information, it takes approximately 30 days to go through the registration and testing process. The SWFT Configuration Guide is available in the Help menu after successful log-in to SWFT.
13. Will the same ECA PKI cert I use to access JPAS work with SWFT?
    a. The Defense Manpower Data Center (DMDC) will implement PKI login in a future release, but at this time it is not available. The same digital identity can be used for logging into JPAS and SWFT.
14. Can I indicate 80 CAGE codes on my SAR?
    a. The SWFT site administrator can assign additional Cage Codes to a SWFT account that he/she manages. Make sure that all additional Cage Codes are marked in the SAR form, and that the SAR has been properly validated by authorized representative of the company that owns the additional cage code(s).
15. How do you add an additional cage code once the SAR is accepted and an account is granted?
    a. You must submit a new SAR to add an additional CAGE code to the account.

16. Has consideration been given to contract with a nationwide third-party vendor, such as NATA Compliance Services (https://www.natacs.aero/) for fingerprint collection?

    a. Not at this time.

17. If your MFO gets the machine and has your Cage Code on it in the future can you get your own machine to submit?

    a. Yes, you will have to register and test the new machine.

18. Does it take specific software to convert the scanned fingerprint cards to the e-FT?

    a. Yes, it takes specific software to convert scanned fingerprint cards. Please refer to https://www.fbibiospecs.org/IAFIS/default.aspx.

19. Can your CAGE code be in two machines, in case one breaks down?

    a. The CAGE code is used for account management in SWFT. The CAGE code is not specifically assigned to a machine. As long as both machines have been registered and tested you may use either machine.

20. Are we required to annotate the e-QIP Request number in the ORI block? I was told that is how OPM matches the fingerprints to the e-QIP

    a. OPM is able to match the fingerprints to investigation using the applicant's SSN. Please refer to the SWFT Configuration Guide for the correct values to be provided in the ORI block. Incorrect ORI will result in rejection of the e-FP submission.

21. Are the SON and SOI company specific?

    a. Electronic fingerprints will be submitted using DISCO's SON and SOI numbers. OPM will reject the submission if it does not have the proper SON and SOI number.

22. What's the status on using armed forces recruiting centers for electronic fingerprinting (eFP)?

    a. We are currently working on an implementation strategy and will keep you posted on our progress.

23. With the proposal to use local Military recruiter machines, will we be able to simply log into their machines using our JPAS cards, and then simply send the prints that way, or will we need to get our CAGE code registered to their machine?

    a. One of the benefits of partnering with the military recruiting stations is that they have the capability to submit electronic fingerprints directly to OPM. For smaller companies or those widely diverse, this will help alleviate some of the economic and logistical challenges of purchasing electronic fingerprint machines. However, fingerprint submissions for the industry must carry the appropriate SON, SOI, ORI and other codes. This may require a change of the scanning device profile, and a subsequent test with the SWFT and OPM. Please refer to the SWFT Configuration Guide.

24. Where do we get the very specific software to be able to simply scan hard copies for conversion to the EFT files?

    a. Refer to the FBI-certified product list for a listing of certified software. Most vendors have accompanying software with their machines so please ensure it meets configuration guidelines. https://www.fbibiospecs.org/IAFIS/Default.aspx

25. Currently submitting hardcopy fingerprint cards, we are required to wait until the investigation reaches a certain stage with OPM. This is not the case with electronic? I heard you say you could submit the fingerprints EFT file before the e-QIP?

    a. Yes you may submit the electronic fingerprints to SWFT before the investigation request is submitted to DISCO. Electronic fingerprint results are valid for 120 days versus the 14 day period when the hardcopy fingerprint card must arrive at OPM to link up with the e-QIP submission.

26. Are we required to submit EFT prior to submitting the SF86?

    a. No, you not required to submit the EFT prior to submitting the SF86.

27. Does the SF86 have to be approved by DISCO before you submit the fingerprints?

a. No, the SF86 does not have to be approved before electronic fingerprint submissions. DISCO recommends uploading the EFT file to SWFT once the SF86 is released to DISCO for review and approval.

28. Do you need a CAGE code for each machine registration or for each company (their cage) that uses it? Why are multiple CAGE codes on the SAR required if the approved machine can scan for any company CAGE?

a. CAGE codes on the SAR are required to identify which companies the account managers are authorized to submit fingerprints. Once the account is created the account managers can register the equipment and software online.

29. Can we digitally sign e-fingerprint files?

a. Digitally signed e-fingerprints files are not supported and will lead to file rejection if submitted to SWFT and OPM.

30. Will there be a shared facility for fingerprinting?

a. The decision to establish a shared facility is up to the Industry community and based on mission areas. DSS does not create shared facilities.