CLASSIFICATION: UNCLASSIFIED

# SWFT PROCEDURE FOR APPROVING THIRD PARTY SERVICE PROVIDERS

## VERSION 1.1

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

**18 July 2023**

# SWFT PROCEDURE FOR APPROVING THIRD PARTY SERVICE PROVIDERS

The *SWFT e-Fingerprint Service Provider's* list serves only as a reference guide to identify SWFT registered service providers for the purposes of electronic fingerprint capture and/or submission. This list neither suggests nor implies any endorsement or preference by the DCSA or the Department of Defense (DoD) about the qualifications or any other aspect of the entities listed. SWFT access requirements outlined by the DCSA must be met prior to listing.

Any business or entity meeting the pre-requisites may request a listing. Pre-requisites and listing application procedures are detailed below. Service providers are limited to the use of SWFT Biometric Upload. All other available connectivity options are for DoD and Federal Agencies only.

To maintain presence on the *SWFT e-Fingerprint Service Provider's* list, the service provider must maintain the pre-requisites and ensure that POC information remains updated with SWFT/DCSA. The list will be audited by DCSA to ensure that the listed providers are in compliance with established system access policies and procedures. Non-compliance will result in account deactivation and removal from the provider list. The service provider may re-apply for listing after the pre-requisites have been met. DCSA reserves the right to deny listings for non-compliance and/or additional security concerns.

## Service Provider Pre-Requisites:

1. **Hardware/Software:** Possess FBI-Approved Scanner Hardware and Software which produces type 4 fingerprints and satisfies EBTS Version 10.x (livescan or cardscan).  The list of FBI certified products and software is available on the FBI website at ***https://fbibiospecs.fbi.gov/certifications-1/cpl***
2. **Access Requirement:** Public Key Infrastructure (PKI) certificate stored on a medium security hardware token, CAC, ECA, PIV or PIV-I.
3. **Clearance/Investigation Level** (FCL or PCL are acceptable)
   Organizations can start the process by reviewing and following the documents, videos and checklist provided by DCSA's Facility Clearance Branch here: https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Facility-Clearances/
   a. **Facility Clearance Level (FCL):** A facility clearance level is the administrative determination that an organization or company is eligible for access to classified information.
      i. Requirements to obtain a FCL:
         1. Obtain a Cage Code through System Award Management (SAM) or DLA.
         2. Be sponsored by either a Government Contracting Activity (GCA) or another cleared defense contracting company.
         3. Have the sponsorship request approved by DCSA to start the FCL process.
         4. Complete the entire FCL process within the allotted timeframe.
   b. **Personnel Clearance Level (PCL):** A PCL is the administrative determination that an industrial employee is eligible for access to classified information.
      i. Requirements to obtain a PCL:
         1. Obtain a Government Contracting Activity (GCA) or another cleared defense contracting company this is willing to sponsor the individual(s).
         2. The ability to pass a background check and maintain a personnel security clearance.

**Listing Requirements:**

1. The following information should be emailed to the DCSAFTSTeam@mail.mil for approval:
   a. Company Name
   b. Company Address – *If there are multiple locations, please provide the main addresses. Additional addresses and locations will be documented during account creation/hierarchy build.*
   c. Point of Contact (POC)/Key Management Personnel (KMP) Name, Title, Address, Email and Phone Number
   d. Company CAGE Code or Federal Agency Name – If another Agency or DOD Cleared Contractor is sponsoring your PCL/FCL, please include the sponsor's name and POC/KMP information (Name, Address, Email and Phone Number).