Requirement Specification

Electronic Fingerprint Data Deliverables

1. Scope of Acquisition

This is a supply contract for the procurement of up to 300,000 formatted, digitized fingerprint data deliverables. The Contractor shall provide finished, compliant electronic fingerprint files delivered directly to the Defense Counterintelligence and Security Agency (DCSA) Fingerprint Transaction System (FTS).

2. Background and Objective

Under the Trusted Workforce (TW) 2.0 Implementation Strategy, DCSA is required to enroll National Security Sensitive personnel into the FBI's Rap Back service. To accomplish this, DCSA requires a "classifiable fingerprint" on file for all subjects.

The objective of this acquisition is to procure these digitized fingerprint data files directly from a commercial vendor. DCSA will separately manage the scheduling, notification, and ultimate Rap Back enrollment of the NISP population. The Contractor's sole objective is to capture, digitize, format, and deliver the fingerprint data to DCSA FTS when subjects utilize the Contractor's footprint.

3. Salient Characteristics (Product Specifications)

To be accepted by the Government, each delivered digitized fingerprint data file must meet the following technical criteria:

3.1 File Formatting & Structural Standards

- All electronic fingerprint files must be formatted as standard .EFT (Electronic Fingerprint Transmission) files, which is the primary and preferred format. Alternatively, .SUB files are authorized as a secondary fallback.
- The generated eFP files must fully comply with the current version of the FBI Electronic Biometric Transmission Specification (EBTS).

3.2 Type-4 Fingerprint Images

In accordance with DCSA FTS requirements, the file must contain a complete set of Type-4 fingerprint images, which strictly consist of:

- 10 rolled impressions (one for each individual finger).
- 1 Plain Left and Right Simultaneous Four-Finger Impression (flat prints).

- 1 Plain Left and Right Thumb Impression.

3.3 FBI Certified Hardware/Software

- All LiveScan or CardScan hardware and software used to capture and compile the biographic/biometric data must be officially listed on the FBI Certified Products List (CPL).

3.4 Identifier Integration

Each data file must successfully integrate the subject's digitized fingerprint with their associated Personally Identifiable Information (PII) and the specific agency identifiers required for accurate routing.

3.5 Secure Transmission & Network Standards

Because these deliverables contain highly sensitive PII, transmissions must utilize secure Department of Defense (DoD) gateways:

- **SWFT System Integration:** Fingerprint files must be uploaded and routed through the Secure Web Fingerprint Transmission (SWFT) web application (or integrated SWFT+ online enrollment systems) to reach the FTS.
- **Device Registration:** Before any data can be transmitted to the production environment, the specific scanning hardware/server platform pair must be successfully registered, tested, and approved by the SWFT Registration Authority.
- **Encryption and Routing:** Data in transit must be protected using Federal Information Processing Standards (FIPS)-compliant encryption and routed through secure, unidirectional virtual private network (VPN) tunnels to DCSA's secure web interfaces.
- **Authentication:** Access and transmission via SWFT require DoD-approved Public Key Infrastructure (PKI) certificates stored on a medium security hardware token (such as a CAC, PIV, PIV-I, or ECA).

4. Delivery Requirements

- **Delivery Mechanism:** Successful electronic transmission and receipt of the data file into the DCSA FTS repository via SWFT.
- **Delivery Schedule:** Deliverables shall be transmitted continually as subjects are processed, with final deliverables completed no later than the date specified in the Delivery Order; 29 September 2026.
- **Invoicing:** The Contractor shall invoice on a Firm-Fixed-Price basis only for the quantity of digitized fingerprint files successfully delivered to and accepted by the DCSA FTS.

5. Inspection and Acceptance

The Government will inspect the deliverables upon receipt at the DCSA FTS.

- **Inspection:** DCSA systems will automatically review the transmitted file for data corruption, formatting errors (ensuring correct .EFT or .SUB structure), EBTS compliance, and missing identifiers.
- **Acceptance:** Acceptance occurs when the system successfully ingests the data file.
- **Defective Supplies:** Defective files (e.g., corrupted data, mismatched PII, or prints rejected by SWFT/FTS for poor quality) will be returned to the Contractor. The Contractor must provide a replacement (a reprint) at no additional cost to the Government.

6. Data Security & Handling Compliance

Because the production of these supplies requires handling Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII), the Contractor must adhere strictly to the following:

- **NIST SP 800-171:** Information systems used to process, store, and transmit the CUI/PII must be fully compliant with NIST Special Publication 800-171.
- **Privacy Act:** All PII handled during the creation of these deliverables must be protected in strict accordance with the Privacy Act of 1974.
- **U.S. Persons Requirement:** Any Contractor personnel who handle PII while generating these supplies must be verified U.S. Citizens.