(U) Fingerprint and Latent Fingerprint Identification Policy Guide

(U) Federal Bureau of Investigation

(U) Criminal Justice Information Services Division

(U) 0973PG

(U) June 14, 2017

(U) Approvals

Policy Information

Date of Last Renewal	N/A
Effective Date	2017-06-14
Review Date	2020-06-14

Approval Information

Sponsoring Executive Approval	Douglas E. Lindquist Assistant Director Criminal Justice Information Services Division
Stakeholder Executive Approval	Christopher Doss Assistant Director Laboratory Division
Final Approval	Christopher M. Piehota Executive Assistant Director Science & Technology Branch

(U) General Information

(U) Questions or comments pertaining to this policy guide can be directed to:

(U) Federal Bureau of Investigation Headquarters,
Criminal Justice Information Services Division

Information Services Branch, Biometric Services Section

(U) Latent fingerprint identification questions or comments pertaining to this policy guide can be directed to: b7E

(U) FBI Headquarters, Laboratory Division

Biometrics Analysis Section, Latent Print Support Unit

(U) Supersession Information

(U) This document supersedes the Fingerprint *and Latent Fingerprint Identification Policy Guide*, 0778PG.

(U) This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the unit or individual(s) listed in the contact section of this policy guide.

(U) Revision Log

(U) The revision log documents substantive changes made to the previous version of the *Fingerprint and Latent Fingerprint Identification Policy Guide*, 0778PG, published on July 20, 2015].

(U) The numbers and titles in the "Revised" column refer to the subsections as they currently appear in this updated policy. Thus, if subsection 2.5. is substantively updated, it would appear as 2.5. in the "Revised" column. "Deleted" subsection numbers refer to those in the previous published version of the policy. When a subsection is removed, subsequent subsections are renumbered. For example, if subsection 2.5. is deleted, subsection 2.6. becomes the new subsection 2.5.

Revised Section Number and Title	Deleted Section Number and Title
4.1.15. (U) Removing the Administrative Burden for Dispositions	5.2. (U) Legal Information for Civil Fingerprint Checks
4.1.15.2. (U) Use of the R-84 by Field Offices	
4.1.15.2.2. (U) Data for Preparing the R-84 Form	
4.2.2.6.1. (U) Letters Submitting Evidence or Articles for Examination	
4.3. (U) Legal Information for Civil Fingerprint Checks	

(U) Table of Contents

1. (U) Introduction 1
1.1. (U) Purpose 1
1.2. (U) Scope 1
1.3. Exemptions 1
2. (U) Roles and Responsibilities 2
2.1. (U) Director of the Federal Bureau of Investigation 2
2.2. (U) Criminal Justice Information Services Division 2
2.2.1. (U) Biometric Services Section (BSS) 2
3. (U) Policy Statement 5
4. (U) Processes and Procedures 6
4.1. (U) Fingerprint Identification 6
4.1.1. (U) Fingerprint Identification Services 6
4.1.2. (U) Next Generation Identification System 6
4.1.3. (U) Summary of the Services of the Criminal Justice Information Services Division 6
4.1.4. (U) Biometric Services Section Customer Service Group 6
4.1.5. (U) Categories of Records in the Next Generation Identification System 7
4.1.6. (U) Access to FBI Criminal History Records 8
4.1.7. (U) Use of Criminal History Record Information for Non-Criminal-Justice Purposes 13
4.1.8. (U) Individual's Right to Access FBI Criminal History Records 15
4.1.9. (U) Notification of Pending Legislation or Project Requests 19
4.1.10. (U) Biographic Submission Data 21
4.1.11 (U) Types of Fingerprint Cards 23
4.1.12. (U) Files in the Criminal Justice Information Services Division 24
4.1.13. (U) Processing of Fingerprint Submissions at the Criminal Justice Information Services Division 26
4.1.14. (U) Certification of Identification Records and Fingerprints 28
4.1.15. (U) Removing the Administrative Burden for Dispositions 28
4.1.16. (U) Acknowledgement of Fingerprints by the Criminal Justice Information Services Division 31

4.1.17. (U) Expungement of Fingerprints by the Criminal Justice Information Services Division 32

4.1.18. (U) Foreign Fingerprints Exchange 32

4.1.19. (U) FBI Literature Concerning Criminal Justice Information Services Division Work and Functions 32

4.1.20. (U) Requests for Copies of Fingerprint Cards 33

4.2. (U) Latent Fingerprint Identification 33

4.2.1. (U) Laboratory Division: Latent Print Units and Programs 33

4.2.2. (U) Procedures and Processes of the Laboratory Division's Latent Print Units 35

4.2.3. (U) Secondary Evidence 39

4.2.4. (U) Requesting Copies of Records (Discoveries) 39

4.2.5. (U) Testimony 39

4.2.6. (U) Services of the Disaster Squad 39

4.3. (U) Legal Information for Civil Fingerprint Checks 40

5. (U) Summary of Legal Authorities 42

(U) List of Appendices

(U) Appendix A: Sources of Additional Information A-1

(U) Appendix B: Contact Information B-1

(U) Appendix C: Definitions and Acronyms C-1

(U) Appendix D: Guidelines for Capturing Palm Prints and Supplementals D-1

1. (U) Introduction

1.1. (U) Purpose

(U) The purpose of the *Fingerprint and Latent Fingerprint Identification Policy Guide* is to provide information about the Criminal Justice Information Services (CJIS) Division's Fingerprint Identification Program (FIP) and the Laboratory Division's (LD) Latent Fingerprint Program.

(U) While this policy guide (PG) is useful as a reference for understanding the activities of the Federal Bureau of Investigation's (FBI) FIP, it is important to note that the performance of many of the procedures described herein requires specialized training and experience.

1.2. (U) Scope

(U) This PG applies to all FBI employees who provide or use fingerprint identification services to identify and investigate individuals, whether for civil or criminal purposes.

1.3. Exemptions

(U) There are no exemptions to this policy.

2. (U) Roles and Responsibilities

2.1. (U) Director of the Federal Bureau of Investigation

(U) According to Title 28 Code of Federal Regulations (CFR) Section (§) 0.85(b), the Attorney General (AG) charges the Director of the FBI to:

> Conduct the acquisition, collection, exchange, classification, and preservation of fingerprints and identification records from criminal justice and other governmental agencies, including fingerprints voluntarily submitted by individuals for personal identification purposes; provide expert testimony in federal, state, and local courts as to fingerprint examinations; and provide fingerprint training, and identification assistance in disasters and for other humanitarian purposes.

2.2. (U) Criminal Justice Information Services Division

(U) CJIS provides leadership for the biometric identification activities of the FBI. The assistant director (AD) of CJIS serves as the liaison between the Director of the FBI and the FIP. The AD also provides program oversight, ensuring that the activities of the FIP meet the overall mission of CJIS, as well as that of the FBI.

2.2.1. (U) Biometric Services Section (BSS)

(U) The BSS provides biometric identification and criminal history services to criminal justice agencies and other authorized entities through the utilization of the Next Generation Identification (NGI) system. Through NGI, the BSS processes criminal electronic ten-print fingerprint identification submissions in [redacted] or less and processes civil electronic fingerprint submissions in [redacted] or less. The BSS updates and maintains CJIS's criminal history database with current information by processing arrest dispositions, wanted notices, expungement notices, and probation/parole flashes. The BSS notifies "wanting" agencies when an applicant submission is identified as having a criminal history with an active wanted notice. The BSS provides the best possible customer service to support NGI customers by handling all inquiries in an efficient and professional manner and provides the highest quality training for current and future biometric initiatives and testimony to the law enforcement and criminal justice communities. The BSS promotes the continuous quality improvement of products and services to meet the ever-changing needs of biometrics. The BSS develops and maintains interagency frameworks that support latent information sharing among federal and international partners in order to enhance national security and uphold the accuracy, integrity, and timeliness of latent services for internal and external users. It provides investigative support to FBI field offices (FO) by comparing facial images of subjects who are the focuses of active field investigations against those housed in selected databases, both internal and external to the FBI. The BSS collaborates with the Biometric Center of Excellence (BCOE) Unit of the Global Operations Section (GOS) to explore and advance the use of new and enhanced biometrics and identity management technologies, along with the capabilities available for integration into operations. The BCOE, a Science and Technology Branch (STB) initiative, sponsors applied research, prototyping, tests and evaluations; participates in standards activities; and hosts collaboration events and training activities related to biometric technologies.

b7E

2.2.1.1. (U) Biometric Support Unit (BSU)

(U) The BSU provides services for law enforcement and authorized non-criminal-justice agencies. The BSU performs criminal history record (CHR) services, name check services, and manual fingerprint file automation and maintenance services. The BSU provides timely and accurate information in support of reducing criminal activity, along with ensuring public safety.

2.2.1.2. (U) Criminal History Information and Policy Unit (CHIPU)

(U) The CHIPU supports the Interstate Identification Index (III) and the National Fingerprint File (NFF) Programs, which includes coordination with states and territories that are making the technical operational changes to join or upgrade participation in the programs. The CHIPU provides administrative support to the National Crime Prevention and Privacy Compact Council (NCPPCC), which includes coordination with the chairperson of the NCPPCC and its committees to:

1. (U) Conduct research and analysis.
2. (U) Perform statistical reviews.
3. (U) Draft and present staff papers.
4. (U) Draft rules and notices for *Federal Register* publications.
5. (U) Work closely with the Office of the General Counsel's (OGC) Criminal Justice Information Law Unit and the CJIS Audit Unit on council initiatives.
6. (U) Provide quality information, services, and solutions to support the interstate exchange of criminal history record information (CHRI) for criminal justice purposes.

(U) The CHIPU responds to a variety of incoming written communications and inquiries from private citizens, law enforcement agencies, law offices, and other professional offices, including congressional offices; supports the FBI LD by providing confirmation of the deoxyribonucleic acid (DNA) profile, the identity of an offender, and the qualifying criminal offense that permits the DNA profile to remain in the National DNA Index System; and processes Departmental Order (DO) 556-73 requests from private citizens who are requesting copies of their CHRs for personal review, to challenge the information on record, to satisfy a requirement for adopting a child in the United States (U.S.) or internationally; or to satisfy a requirement to live, work, or travel in a foreign country (e.g., police certificate, letter of good conduct, or criminal history background).

(U) The CHIPU also researches CHRI and communicates with all types of law enforcement agencies to obtain arrest and disposition information in an effort to make CHRI as complete as possible and to liaise with local, state, federal, tribal, and international agencies for the purposes of obtaining and improving disposition and other CHRI.

2.2.1.3. (U) Customer Support Unit (CSU)

(U) The CSU serves as the central point of contact (POC) for internal and external customers of the BSS. The CSU provides internal support by ensuring system availability and database integrity; delivering functional training; facilitating system and process improvements; creating

functional policies and procedures; coordinating space and equipment matters; and developing strategic management tools. Externally, the CSU provides liaison services to local, state, federal, tribal, and international criminal justice and non-criminal-justice agencies, as well as to U.S. citizens and non-U.S. persons (USPER). Additionally, the CSU supplies written testimony, verbal testimony, and certified copies of criminal history information for use in legal proceedings.

2.2.1.4. (U) Facial Analysis Comparison and Evaluation (FACE) Services Unit

(U) The FACE Services Unit provides investigative support to the field by comparing facial images of subjects who are the focuses of active FBI investigations against those housed in selected databases that are both internal and external to the FBI. The FACE Services Unit receives facial images (probes) from the field, conducts face searches of all appropriate and available facial recognition systems, compares probe images against the images on the resulting candidate lists, and provides feedback to requesting agents of those candidates deemed most-likely matches to their subjects. The FACE Services Unit also utilizes case information provided with probe images to conduct text-based searches in order to locate additional photos and to provide information that can be used as an investigative tool. This face service will be expanded to include a larger customer base as the operation evolves.

2.2.1.5. (U) Latent and Forensic Support Unit (LFSU)

(U) The LFSU serves as CJIS's liaison to authorized law enforcement and national security agencies by providing research, analytical, and project management support. The LFSU's subject matter expertise allows users to leverage existing latent, palm-print, and ten-print services, as well as new services and technologies to prevent and solve crimes, while upholding the accuracy and timeliness of such services. The LFSU is committed to enhancing the existing investigative and identification capabilities of both criminal and non-criminal-justice agencies and enabling a more comprehensive approach to public safety, law enforcement, and intelligence efforts.

2.2.1.6. (U) Quality Improvement Unit (QIU)

(U) The QIU is committed to organizational strategic thinking, decisions, and results, as well as the enhancement of biometric identification and CHR maintenance through the use of tools such as postprocess review, sampling, updating procedures, and statistical data analysis. These commitments ensure that CJIS maintains consistency and remains customer-focused.

3. (U) Policy Statement

(U) The FBI operates its FIP pursuant to federal statutes and regulations. Together, CJIS and the LD manage the FBI FIP, which serves to:

1. (U) Acquire, collect, exchange, classify, and preserve fingerprints and CHRI from criminal justice and other government agencies, including fingerprints voluntarily submitted by individuals for personal identification purposes.
2. (U) Provide expert testimony concerning fingerprint examinations in federal, state, local, and tribal courts.
3. (U) Conduct fingerprint training.
4. (U) Assist with identifications in disasters and for other humanitarian purposes.

(U) Through fingerprint identification, CJIS delivers timely and relevant law enforcement and criminal justice information about individuals to the FBI and qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

(U) The LD is responsible for the receipt, management, and disposition of all latent fingerprint evidence received for forensic examination.

4. (U) Processes and Procedures

4.1. (U) Fingerprint Identification

4.1.1. (U) Fingerprint Identification Services

(U) Federal statutes authorize the FBI to acquire, collect, classify, and preserve identification, criminal identification, crime, and other records, as well as any information that would assist in the identification of deceased individuals or the location of missing persons and to exchange such records and information with, and for official use by, authorized officials of the federal government, including the United States Sentencing Commission and state, city, penal, and other institutions.

4.1.2. (U) Next Generation Identification System

(U) In 2014, the NGI system officially replaced the legacy Integrated Automated Fingerprint Identification System (IAFIS) and provided new functionality. The NGI advanced fingerprint identification technology provides faster, more efficient identification processing, increased search accuracy, and improved latent processing services.

4.1.3. (U) Summary of the Services of the Criminal Justice Information Services Division

(U) CJIS's fingerprint identification and CHRI services include, but are not limited to:

1. (U) Processing criminal, law enforcement/criminal justice, applicant, and personal identification ten-print submissions. Identification information submitted for reasons other than law enforcement/criminal justice will be processed for a fee.
2. (U) Placing dispositions, expungements, specialty documents, miscellaneous documents, wanted notices, flash notices, and missing person notices into CJIS's records and/or systems.
3. (U) Handling fingerprint submissions for international searches.
4. (U) Providing ten-print records testimony.

(U) CJIS established the Training and Records Testimony Team (TRTT) to be responsible for developing policies and procedures for the Ten-Print Records Testimony Program. The majority of records testimonies fulfilled through the TRTT describe the fingerprint comparisons of known-to-known subjects and may exclude the fingerprints of individuals with CHRs. Testimony concerning latent fingerprints or LD responsibilities is not provided by the TRTT.

4.1.4. (U) Biometric Services Section Customer Service Group

(U) BSS representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. by calling (304) 625-5590. For calls made after hours, a message may be left, and a customer service representative will return the call on the next business day.

4.1.5. (U) Categories of Records in the Next Generation Identification System

(U) The records in the NGI system include fingerprints and palm prints; corresponding criminal histories; mug shots; scar and tattoo photos; physical characteristics such as height, weight, hair and eye color; and aliases. The system also includes civil fingerprints, most of which are from individuals who have served or are serving in the U.S. military or who have been or are employed by the federal government. The fingerprints and CHI is submitted voluntarily by state, local, federal, tribal, and international law enforcement agencies.

4.1.5.1. (U) Six-Key Next Generation Identification Services

4.1.5.1.1. (U) Ten-Print-Based Fingerprint Identification Services

(U) A ten-print fingerprint submission contains ten rolled fingerprint impressions and corresponding flat fingerprint impressions.

(U) Criminal ten-print fingerprint submissions: Fingerprints are acquired as the result of an arrest at the city, county, state, or federal level. The fingerprints are processed locally and then electronically forwarded to a state or federal agency system for processing. The fingerprints are then sent through the CJIS wide-area network (WAN) to the NGI for processing.

(U) Civil ten-print fingerprint submissions: Fingerprints are acquired for background checks for employment, licensing, or other non-criminal-justice purposes, where authorized by federal and state laws and in compliance with appropriate regulations. To determine what occupations are authorized within a specific state, contact the state police or the state criminal history repository. Similar to criminal fingerprints, civil fingerprints are processed by local, state, or federal agencies prior to being submitted to the NGI for processing.

4.1.5.1.2. (U) *Latent Fingerprint Services*

(U) The NGI supports both electronic and hard-copy submissions of latent fingerprints. It provides the FBI Laboratory with enhanced search capabilities, using databases specially designed for matching latent fingerprints. Latent fingerprint specialists return decisions to requestors and add any unidentified latent fingerprints and their features to the Unsolved Latent File (ULF).

4.1.5.1.3. (U) Subject Search and Criminal History Services

(U) The III segment of the NGI is the national system designed to provide automated CHRI. The III stores the CHRI of federal offenders and those offenders established by participating and nonparticipating III states. Each record is created through the submission of fingerprint images to NGI. The participating states establish and update records within the III through the submission of first and subsequent fingerprint images of arrested subjects. Once these records are established, the participating states provide requested CHRs when an electronic inquiry for a state-maintained record is processed by the system.

(U) States in the final stage of the III, as NFF participants, submit only the first arrest fingerprint images of a subject to establish a pointer record within the index segment. Any subsequent activity related to this NFF pointer record will be the sole responsibility of the NFF-participating state. If a direct-terminal inquiry or an NGI fingerprint inquiry identifies a person with a criminal

history in one or more NFF-participating states, a criminal-history request will be forwarded to the participating NFF state's criminal history system for the appropriate response.

4.1.5.1.4. (U) Document and Imaging Services Document Services

(U) The NGI processes documents associated with CHR received in electronic, hard-copy, or machine-readable data formats. These documents include arrest dispositions, expungements, and other miscellaneous updates.

(U) Fingerprint image services: Upon request, the NGI supplies electronic images of fingerprints to authorized agencies. See the Electronic Biometric Transmission Specification (EBTS) at [redacted] subsections 3.6-3.7, for more information. b7E

(U) Photo services: The NGI has the capability to accept, store, and distribute photos. See Appendix K of the EBTS for information regarding photo submissions and subsection 3.10 for photo retrievals.

4.1.5.1.5. (U) Remote Ten-Print and Latent Fingerprint Search Services

(U) The NGI supports remote ten-print and latent fingerprint searches by law enforcement agencies. The results of remote ten-print and latent searches are returned electronically and include a list of potential matching candidates and corresponding fingerprints for comparison and identification by requesting agencies.

(U) The FBI will provide the following remote search software packages to criminal justice agencies upon request and free of charge.

1. (U) Remote Fingerprint Editing Software (RFES): This complete software package performs remote searches of NGI. RFES supports remote NGI transactions, including images and feature-based searches for both ten-print and latent fingerprints. RFES editing and human interface were developed based on use and the advice of both local law enforcement and FBI latent fingerprint specialists.
2. (U) Universal Latent Workstation Software: The Universal Latent Workstation Software package performs remote latent searches of the NGI. (For additional information regarding Universal Latent Workstation, see [redacted] b7E

4.1.6. (U) Access to FBI Criminal History Records

(U) Access to FBI CHRs is made available to the following entities:

1. (U) Criminal justice agencies, for criminal justice purposes. [Title 28 United States Code (U.S.C.) Section (§) 534; 28 CFR § 20.33(a)(i)]
2. (U) Non-criminal-justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies. [28 CFR § 20.33(a)(6)]
3. (U) Private contractors, for the purpose of providing services for the administration of criminal justice pursuant to a specific agreement with (1) a criminal justice agency, or (2) a non-criminal-justice governmental agency performing criminal justice dispatching

functions or data processing/information services for a criminal justice agency. (The agreement between the agency and the private contractor must incorporate an AG-approved security addendum that specifically authorizes access to CHR information; limits the use of the information to the purposes for which it was provided; ensures the security and confidentiality of the information, consistent with existing regulations; provides for sanctions; and contains such other provisions, as the AG may require. The power and authority of the AG on these matters must be exercised by the Director of the FBI or the Director's designee). [28 CFR § 20.33(a)(7)]

4. (U) Officials of civil or criminal courts, for use only in domestic violence or stalking cases. [Violent Crime Control and Law Enforcement Act of 1994, Public Law (Pub. L.) 103-322; 28 U.S.C. § 534]

5. (U) Officials of (1) the National Center for Missing and Exploited Children (NCMEC), to be used only within the scope of the center's duties and responsibilities under federal law to assist or support law enforcement agencies in the administration of criminal justice functions, and (2) governmental social service agencies with child-protection responsibilities, to be used by such agencies only in investigating or responding to reports of child abuse, neglect, or exploitation. [Adam Walsh Child Protection and Safety Act of 2006, Pub. L. 109-248 § 151; 42 U.S.C. § 1696]

6. (U) Officials of federally chartered or insured banking institutions, to promote or maintain the security of those institutions and, if authorized by state statute and approved by the AG of the United States, to officials of local and state governments for purposes of non-criminal-justice employment and licensing. [Pub. L. 92-544; 28 U.S.C. § 534 Note, 86 Stat 1115]

7. (U) The Department of Defense (DoD); U.S. Department of State; Department of Transportation (DOT); Office of Personnel Management (OPM); FBI; or the Central Intelligence Agency (CIA), to determine the eligibility of a person for access to classified information; assignment to, or retention in, sensitive national security duties; acceptance or retention in the armed forces; and appointment, retention, or assignment to a position of public trust or a critical or sensitive position while either employed by the government or performing a government contract. [5 U.S.C. § 9101]

8. (U) Federal agencies, for use in conducting background checks of present and prospective employees, including employees of childcare centers at any facility operated or under contract by the federal government. [Executive Order (EO) 10450; Crime Control Act of 1990, Pub. L. 101-647; 42 U.S.C. § 13041]

9. (U) Officials of state racing commissions, to conduct background checks of applicants for state licenses to participate in parimutuel wagering in states with a state statute approved under Pub. L. 92-544. [Parimutuel Licensing Simplification Act of 1988, Pub. L. 100-413; 102 Stat. 1101; 28 U.S.C. § 5344 Note]

10. (U) Officials of tribal governments, to conduct background checks of applicants for employment who would be in positions involving regular contact with, or having control

over, Native American children in such tribes. [Indian Child Protection and Family Violence Prevention Act, Pub. L. 101-630, 25 U.S.C. §§ 3205 and 3207]

11. (U) The FBI and local/state agencies, acting as POCs for the National Instant Criminal Background Check System, that are permitted full access to the III for the purpose of determining if an applicant is prohibited from purchasing or redeeming a firearm from pawn, as provided in the Brady Handgun Violence Prevention Act. Additionally, criminal justice officials may use III for making firearms- or explosives-related background checks when required to issue firearms- or explosives-related licenses or permits according to state statutes or local ordinances. [Fingerprints submitted for the non-criminal-justice purpose of issuance of firearms and related permits are processed pursuant to Pub. L. 92-544, Brady Handgun Violence Prevention Act, Pub. L. 103-159; 18 U.S.C. § 922 and 28 CFR Part 25.]

12. (U) Officials of the Securities and Exchange Commission (SEC) and self-regulatory organizations designated by the SEC, for use in conducting fingerprint-based background checks of all partners, directors, officers, and employees of national securities exchanges; brokers; dealers; registered transfer agents; registered clearing agencies; registered securities information processors; national securities exchanges; and national securities associations. [Securities Acts Amendments; Pub. L. 94-29, amended by Pub. L. 100-181 15 U.S.C. § 78q(f)(2)]

13. (U) Officials of the Commodity Futures Trading Commission (CFTC) and the National Futures Association (NFA), for background checks of applicants for registration with the CFTC (e.g., NFA commission merchants, introducing brokers, commodity trading advisors, commodity pool operators, floor brokers, and associated persons). [Futures Trading Act of 1982, Pub. L. 97-444; 7 U.S.C. § 21(b)(4)(E); and 7 U.S.C. § 6k(1)]

14. (U) Officials of the Nuclear Regulatory Commission, for background checks of individuals permitted unescorted access to nuclear utilization facilities or permitted access to safeguard information. [Omnibus Diplomatic Security and Antiterrorism Act of 1986, Pub. L. 99-399; 42 U.S.C. § 2169]

15. (U) Officials of the Department of Homeland Security (DHS) Transportation Security Administration (TSA), who must coordinate with airport operators and air carriers to conduct background checks of (1) persons who have escorted and unescorted access or who may permit others to have unescorted access to aircraft of a U.S. air carrier or a foreign air carrier or to a secured area of an airport that serves an air carrier; (2) persons responsible for screening their supervisors and passengers or property; and (3) persons who exercise security functions associated with baggage or cargo. [Aviation Security Improvement Acts of 1990 and 2000, Pub. L. 101-604 and Pub. L. 106-272; amended by Aviation and Transportation Security Act, Pub. L. 107-71; 49 U.S.C. §§ 44935-44936; and 49 CFR § 1542.209]

16. (U) Public Housing Authorities, in the implementation of the Housing Opportunity Program Extension Act of 1996, may request criminal conviction records on adult applicants for, or tenants of, public housing for the purposes of applicant screening, lease

enforcement, or eviction. [Housing Opportunity Program Extension Act of 1996, Pub. L. 104-120 and Pub. L. 105-276, 42 U.S.C. § 1437d(q)]

17. (U) Tribes or tribally designated housing entities, in the implementation of the Native American Housing Assistance and Self-Determination Act of 1996, may request criminal conviction records of adult applicants for, or tenants of, housing assisted with grant amounts provided to such tribes or entities under this act for the purposes of applicant screening, lease enforcement, or eviction. [Native American Housing Assistance and Self-Determination Act of 1996, Pub. L. 104-330, 26 U.S.C. § 4138]
18. (U) Nursing facilities and home health care agencies, for background checks on applicants for employment in direct patient care. [Pub. L. 105-277, 28 U.S.C. § 534 Note]
19. (U) Officials of state and local governments, for conducting background checks of current and prospective employees or volunteers who provide or will provide care to children, the elderly, or individuals with disabilities, in the absence of a state statute approved under Pub. L. 92-544. [National Child Protection Act/Volunteers for Children Act, Pub. L. 105-251]
20. (U) Officials of state or local governments, for conducting background checks of potential employees of private prisoner transport companies. [Interstate Transportation of Dangerous Criminals Act of 2000 (Jeanna's Act), Pub. L. 106-560; 42 U.S.C. 13726b; 28 CFR Part 97]
21. (U) Officials of state and local governments, for conducting background checks of employees or applicants for employment as private security officers. [Private Security Officer Employment Authorization Act of 2004, Pub. L. 108-458, Sec. 6402; 28 CFR Part 105, Subpart C]
22. (U) Upon the request of the chief executive officer of a state or officials of a state or local child welfare agency, for the purposes of (a) conducting background checks on individuals under consideration as prospective foster or adoptive parents or (b) conducting an investigation relating to an incident of abuse or neglect of a minor, or (c) a public or private elementary or secondary school or a local or state educational agency on individuals employed by, under consideration for employment by, or otherwise in a position in which the individual would work with or around children in the school or agency. [Adam Walsh Child Protection and Safety Act of 2006, Pub. L. 109-248, Sec. 153; 42 U.S.C. § 16962]
23. (U) Officials of state and local governments, for conducting background checks of persons involved in producing or manufacturing REAL ID driver's licenses and identification cards or persons who have the ability to affect the identity information that appears on such licenses or identification cards. [REAL ID Act of 2005, Pub. L. 109-13, 6 CFR § 37.45]
24. (U) Officials of the Conference of State Bank Supervisors, for use by state regulators and other authorized agencies with approved access to the National Mortgage Licensing

System and Registry to license and/or register mortgage loan originators. [S.A.F.E. Mortgage Licensing Act of 2008, Title V, Pub. L. 110-289]

25. (U) Officials of state and local governments, for use in conducting background checks (pursuant to regulations and requirements established by the Corporation for National and Community Service) on individuals selected by national service program entities who receive a living allowance, a stipend, a national service education award, or a salary through a program receiving assistance. [Serve America Act, §§1612 and 1614, Pub. L. 111-13; 42 U.S.C. § 12645g; 45 CFR Part 2540]
26. (U) Officials of the designated grantee state agency, for use in conducting background checks on direct-access employees of long-term care facilities or providers in grantee states approved by the Center for Medicare and Medicaid Services. [Patient Protection and Affordable Care Act; Pub. L. 111-148, Sec. 6201; 42 U.S.C. § 1320a-71]
27. (U) Officials of state and local governments, for the purpose of court-appointed special advocate programs conducting fingerprint-based background checks of prospective volunteers. [Violence Against Women Reauthorization Act of 2005, Pub. L. 109-162, Sec. 112; 42 U.S.C. § 13013(d)]
28. (U) Officials of the state Department of Health and Human Services, for conducting fingerprint background checks of providers of medical services and suppliers, according to the risk of fraud, waste, and abuse. [Patient Protection and Affordable Care Act. [(Pub. L. 111-148), Sec. 6401; 42 U.S.C. § 1395cc; 42 CFR Part 455]
29. (U) The White House (the President, the Vice-President, their staffs, and those entities of the Executive Offices of the President not subject to the Freedom of Information Act or the Privacy Act), for employment, security, and access purposes compatible with the law enforcement purposes for which they were collected.
30. (U) Local, state, tribal, federal, joint, or other criminal or non-criminal-justice public authority; a foreign or international agency/organization consistent with international treaties, conventions, and/or executive agreements; or other necessary and appropriate entities or individuals in order to enable the FBI, the CIA, or another entity or individual with an intelligence function or mission to carry out lawful intelligence responsibilities under pertinent statutes, EOs, national security directives, AG procedures, or other applicable authorities.
31. (U) Members of the news media or of the general public, in furtherance of a legitimate law enforcement or public safety function.
32. (U) A member of Congress or congressional staff, acting on behalf of the member, who requests such information on behalf of the individual who is the subject of the record.
33. (U) The National Archives and Records Administration (NARA) and the General Services Administration (GSA), for records management inspections and such other purposes conducted under the authority of 44 U.S.C. §§ 2904 and 2906, to the extent that such legislation requires and authorizes the disclosure.

34. (U) Federal agencies authorized to receive them pursuant to federal statute or EO.
35. (U) The FBI, for security risk assessments of individuals who possess, use, or transport select biological agents and/or toxins. [Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. 107-188; 42 U.S.C. § 262, et seq.]

4.1.7. (U) Use of Criminal History Record Information for Non-Criminal-Justice Purposes

(U) The National Crime Prevention and Privacy Compact Act of 1998 (42 U.S.C. § 14611, et seq.) established a 15-member Compact Council (CC) that has the authority to promulgate rules and procedures for the use of the III for non-criminal-justice purposes. The CC includes one member nominated by the FBI Director who is an FBI employee. Additionally, the Director appoints an FBI compact officer who is responsible for administering the CC. The CC requires that fingerprints or other approved forms of positive identification be submitted for all requests of CHRI for non-criminal-justice purposes. The CC has approved the use of both rolled and flat fingerprints as positive identification for non-criminal-justice purposes.

4.1.7.1. (U) Unauthorized Disseminations Involving Agencies and Individuals

(U) Classified and sensitive information in FBI information systems that includes personally identifiable information (PII) must be safeguarded against unauthorized disclosure (see *Privacy Policy Guide*, 0229PG). [redacted] b7E

[redacted] This will also enable FBI compliance with the requirement that incidents involving PII be reported to the Department of Justice Computer Emergency Response Team (DOJCERT) within [redacted] of the discovery of the loss.

4.1.7.1.1. (U) Identify, Report, and Mitigate the Risk of Personally Identifiable Information Breaches

(U//~~FOUO~~) The term PII refers to information that distinguishes an individual, including name, date of birth (DOB), social security number (SSN), or similar information. A PII breach can occur when (1) unauthorized persons or agencies have access to PII, or (2) the location of a document that contains PII is unknown, which could potentially lead to identity theft. PII must be safeguarded against unauthorized disclosure. The CJIS BSS reports possible PII breaches to CJIS's CSO [redacted] b7E

(U) The following are some of the steps that must be taken to mitigate the risk to PII:

1. [redacted] b7E
2.
3.

4.
5.
6.
7.
8.
9.
10.
11.
12.
13.

b7E

4.1.7.1.2. (U) Reporting and Mitigation Efforts of Potential Personally Identifiable Information Breaches

(U) The BSS PII POCs research all potential PII breaches [redacted] A tracking mechanism monitors the PII [redacted] in order to ascertain any operational or employee development issues that need to be addressed. b7E

(U) In the case of a [redacted] incident: b7E

1. (U//~~FOUO~~) [redacted]

2. (U//~~FOUO~~) Customer contacts will be made at the unit chief (UC)-level to ensure that proper discussions are conducted with the affected parties, with no mention of the details [redacted] b7E
3. (U//~~FOUO~~) If requested, the BSS will provide a follow-up response to the customer. This response must be sent to the customer [redacted]
4. (U//~~FOUO~~) BSS will waive the processing fee if a second DO 556-73 request is needed.

4.1.7.1.3. (U) Training and Accountability Measures

(U) The BSS has implemented the following employee training and accountability measures:

1. (U//~~FOUO~~) The CJIS Security and Professional Responsibility Office (CSPRO) meets with all employees assigned to the BSS functions where potential PII breaches have been historically reported [redacted] and provides a security briefing. b7E
2. (U//~~FOUO~~) The BSS has developed a specialized training class to educate the BSS staff regarding PII. This class is mandatory for all new employees assigned to the BSS.
3. (U//~~FOUO~~) If a BSS employee processing error results in a [redacted] incident, a mandatory security awareness briefing must be given to the employee by the CSPRO.
4. (U//~~FOUO~~) The BSS has defined PII as information that can be used to uniquely identify, contact, or locate a single person or information that can be used with other sources to uniquely identify a single individual. The incorrect disclosures that distinguish an individual are name, DOB, SSN, or universal control number (UCN) (formerly FBI number). An employee assumes full accountability for errors related to the incorrect disclosure of PII. An employee completes an accountability form that documents his or her actions and the impact to the customer, the FBI, and the employee and describes how he or she will prevent a breach in the future. The form allows the supervisor to create an action plan with a list of any steps taken to prevent future breaches. These steps are enforced through the employee's performance appraisal. The rating/reviewing official may request that the employee be reevaluated if he or she feels additional training is needed.

(U) The FBI continues to monitor work processes and modify procedures to ensure that classified and sensitive information in FBI information systems that contain PII be safeguarded against unauthorized disclosure.

4.1.8. (U) Individual's Right to Access FBI Criminal History Records

4.1.8.1. (U) Access to the Record

(U) Under 28 CFR §§ 16.30-16.34, any individual may obtain a copy of his or her FBI CHR by submitting a DO 556-73 request for personal review, to challenge the information on record, to satisfy a requirement for adopting a child in the United States or internationally, or to satisfy a requirement to live, work, or travel in a foreign country (e.g., police certificate, letter of good conduct, or criminal history summary). The [redacted] and the [redacted] are both internal forms that are generated from CJIS's b7E

[redacted] application within the NGI system after the processing of a DO request is completed and the results become available. This form letter is already populated with customer information previously entered into [redacted] and is automatically generated, upon completion, directly to CJIS's Service Center for printing and mailing without human intervention [redacted] b7E

(U) Local agencies are usually available to fingerprint persons for employment, licensing, and other purposes; however, where fingerprinting services are not otherwise available, the FO should fingerprint the person. Information regarding the DO 556-73 can be found at <www.fbi.gov>.

4.1.8.2. (U) Challenges to Information

(U) Under 28 CFR §§ 16.30-16.34, the subject of a CHR may challenge the FBI as to the accuracy or completeness of any identifiable entry on that record. The FBI will forward the challenge to the agency that submitted the data and request that the agency verify or correct the challenged entry. The FBI's CJIS Division serves as the nation's central repository and custodian for fingerprints and related Identity History Summary (IdHS) information. As the custodian of such information, CJIS does not have the authority to modify any IdHS information unless specifically notified to do so by the agency that owns the information. If an individual believes his or her IdHS contains inaccurate or incomplete information, the individual has two options for requesting a change or a correction:

1. (U) **Option 1**: Contact the agency or agencies that submitted the information to the FBI.
   - (U) Missing or incorrect state (nonfederal) information:
     - (U) Most states, through agreement with the FBI, require that modification requests for IdHS information be processed through their respective state central repositories (state identification bureaus) before any updates can be applied to FBI records. Individuals may contact their respective state repositories for assistance and, if applicable, request that they provide the FBI with updates to their IdHSs. Contact information for each state is provided on the "State Identification Bureau Listing" at <www.fbi.gov/services/cjis/identity-history-summary-checks/state-identification-bureau-listing>.
     - (U) Several states maintain their own records systems. Records updates are made at the state level only, so the FBI cannot modify its records. Instead, the FBI accesses a state's system for authorized purposes to review a record. Contact information for states maintaining records at the state level is provided on the "State-Maintained Records Listing" at <www.fbi.gov/services/cjis/identity-history-summary-checks/state-maintained-records-listing>.
   - (U) Missing or incorrect federal information:

- (U) For a federal IdHS update, the FBI must receive a request directly from the original arresting agency, from a court with jurisdiction over the arrest data, or from another agency with jurisdiction over the arrest data.

2. (U) **Option 2**: Send a written challenge request to CJIS.

   (U) An individual's written request should clearly identify the information that he or she feels is inaccurate or incomplete, and should include copies of any available proof or supporting documentation to substantiate the claim. For example, if disposition information is incorrect or missing, the individual may submit documentation obtained from the court having jurisdiction over the arrest or the office prosecuting the offense. The FBI will contact appropriate agencies in an attempt to verify or correct challenged entries on the individual's behalf. Upon receipt of an official communication from the agency with jurisdiction over the data, the FBI will make the appropriate changes and notify the individual of the outcome.

   (U) An individual may submit an IdHS challenge to CJIS by writing to the following address:

   FBI CJIS Division
   Attention: Criminal History Analysis Team 1
   1000 Custer Hollow Road
   Clarksburg, WV 26306

4.1.8.3. (U) Unauthorized Disseminations–Individuals

(U//~~FOUO~~) It is the policy of the FBI that PII contained within classified and sensitive information in FBI information systems be safeguarded against unauthorized disclosure. [redacted] b7E

[redacted] This will also help to ensure FBI compliance with the requirement that incidents involving PII be reported to the DOJCERT within [redacted] of the discovery of the loss.

4.1.8.3.1. (U) Identify, Report, and Mitigate the Risk of Personally Identifiable Information Breaches

(U//~~FOUO~~) The term PII refers to information that distinguishes an individual, including, but not limited to, name, DOB, and SSN. A PII breach can occur when (1) unauthorized persons or agencies have access to PII, or (2) the location of a document that contains PII is unknown, which could potentially lead to identity theft. PII must be safeguarded against unauthorized disclosure. The BSS reports possible PII breaches to CJIS's CSO [redacted] b7E

(U) The following are some of the required steps taken to mitigate the risk to PII:

1. [redacted] b7E
2.

3. b7E
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.

4.1.8.3.2. (U) Reporting and Mitigation Efforts of Potential Personally Identifiable Information Breaches

(U) The BSS PII POCs research all potential PII breaches The tracking mechanism monitors the PII in order to ascertain any operational or employee development issues that need to be addressed. b7E

(U) In the case of a incident:

1. (U//~~FOUO~~) b7E

2. (U//~~FOUO~~) Customer contacts are made at the UC-level to ensure that proper discussions are conducted with the affected parties, with no mention to the details [redacted] b7E
3. (U//~~FOUO~~) If requested, the BSS will provide a follow-up response to the customer. This response is sent to the customer [redacted]
4. (U//~~FOUO~~) The BSS will waive the processing fee if a second DO 556-73 request is needed.

4.1.8.3.3. (U) Training and Accountability Measures

(U) The BSS has implemented the following employee training and accountability measures:

1. (U//~~FOUO~~) The CSPRO meets with all employees assigned to the BSS functions where potential PII breaches have been historically reported [redacted] and provides a security briefing. b7E
2. (U//~~FOUO~~) The BSS has developed a specialized training class to educate the BSS staff regarding PII. This class is mandatory for all new employees assigned to the BSS.
3. (U//~~FOUO~~) If a BSS employee processing error results in a [redacted] incident, a mandatory security awareness briefing must be given to the employee by the CSPRO.
4. (U//~~FOUO~~) The BSS has defined PII as information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. The prohibited disclosures that distinguish an individual are name, DOB, SSN, or UCN. An employee assumes full accountability for errors related to the prohibited disclosure of PII. An employee completes an accountability form that documents his or her actions and the impact to the customer, the FBI, and the employee and describes how the employee will prevent a breach in the future. The form allows the supervisor to create an action plan with a list of any steps taken to prevent future breaches. These steps are enforced through the employee's performance appraisal. The rating/reviewing official may request that the employee be reevaluated if he or she feels additional training is needed.

(U//~~FOUO~~) The FBI continues to monitor work processes and modify procedures to ensure that classified and sensitive information in FBI information systems that include PII be safeguarded against unauthorized disclosure.

4.1.9. (U) Notification of Pending Legislation or Project Requests

4.1.9.1. (U) Pending Legislation

(U) FBI FOs must notify FBI Headquarters (FBIHQ), Attention: CJIS Division, of any pending legislation that might curtail or restrict the legal right of local, state, or tribal criminal justice officials to fingerprint arrested persons.

4.1.9.2. (U) Project Requests

(U) FBI FOs must advise CJIS of any requested fingerprint projects. Information concerning the availability of such services must be addressed to FBIHQ, Attention: CJIS Division. FOs may

not make any commitments to handle any "projects" involving the submission of fingerprints to CJIS, unless authorized by CJIS in writing (e.g., e-mail from a designated executive manager).

4.1.9.3. (U) Recording Electronically Submitted Images

(U) CJIS accepts electronically submitted fingerprint images in accordance with the current EBTS standards available at <www.fbibiospecs.org>.

4.1.9.3.1. (U) Common Errors Preventing the Capture of Legible Fingerprints

(U) The common errors that prevent the capture of legible fingerprints include:

1. (U) Failing to properly clean equipment or the hands to be fingerprinted before scanning the fingers.
2. (U) Failing to roll the impressions from nail to nail fully.
3. (U) Failing to roll the impressions in the correct finger blocks.
4. (U) Applying too much or too little pressure when rolling the fingers.
5. (U) Allowing the fingers to slip or twist while rolling, resulting in distorted images.
6. (U) Taking fingerprints of fingers that are excessively moist due to excessive perspiration.
7. (U) Taking fingerprints of fingers that are excessively dry.
8. (U) Failing to recognize and enhance ridge details of individuals who have worn ridge details resulting from occupational or skin conditions or failing to properly use recommended products by not following the vendor's specifications.

4.1.9.4. (U) Major Case Prints

(U) CJIS accepts electronically submitted fingerprint images in accordance with the EBTS, available at <www.fbibiospecs.org>. Additionally, palm print and supplemental fingerprint impressions may be submitted using the FD-884 ("Palm Print") and FD-884a ("Supplemental Finger and Palm Print") forms.

4.1.9.4.1. (U) Procedures for Capturing Palm Prints and Supplementals

(U) The FBI has implemented palm print and supplemental print search capabilities as part of its NGI. FD-884 ("Palm Print") and FD-884a ("Supplemental Finger and Palm Print") forms are available for submitting palm prints and supplementals. Existing cards will be accepted; however, the capture of friction ridge information must be oriented as depicted in Appendix E of this PG.

(U) Ordering information: To order FD-884 (7-02-10) ("Palm Print") and FD-884a (7-02-10) ("Supplemental Finger and Palm Print") form cards at no charge, contact the Fingerprint Supply Center at 304-625-3983 [redacted] b7E

(U) For additional ordering questions, contact the Customer Service Group by telephone at 304-625-5590 or via e-mail at liaison@leo.gov.

(U) Submit a request to CJIS for "Guidelines for Capturing Palm Prints and Supplementals," or send comments regarding palm print cards.

4.1.9.5. (U) Live-Scan Electronically Produced Fingerprint Impressions

(U) If criminal fingerprints are taken with a live-scan device, FBI FOs must submit them electronically. Electronically submitted criminal prints must be in accordance with CJIS Division guidelines, as outlined in the EBTS and available at <www.fbibiospecs.org>.

4.1.10. (U) Biographic Submission Data

4.1.10.1. (U) Biographic Data Submitted by the FBI

4.1.10.1.1. (U) Subjects Incidental to Arrest

(U) FBI FOs must submit biographic information in conjunction with the electronic submission of fingerprints. Electronically submitted criminal prints should be in accordance with the CJIS Division guidelines outlined in the EBTS and available at <www.fbibiospecs.org>.

4.1.10.1.2. (U) Criminal Inquiry

1. (U) Identify the subject as "Criminal Inquiry" in the space marked "Charge."
2. (U) If an identification is made with a previous arrest record, a copy of the record will be furnished to the FBI FO.

4.1.10.1.3. (U) Juveniles

(U) Juveniles may be fingerprinted in accordance with the provisions of 18 U.S.C. § 5038(a).

b7E

b7E

[redacted]

4.1.10.2. (U) FBI Applicants

(U) FBI applicants are fingerprinted at the time of their personnel security interviews. Fingerprints are to be submitted electronically via the Civil Applicant System (CAS) to the [redacted] CJIS Division, West Virginia Complex, Clarksburg, West Virginia, 26306 when a background investigation is initiated. In every instance, FBI personnel must fingerprint applicants for FBI positions. b7E

4.1.10.3. (U) Fingerprints Submitted by Another Criminal Justice Agency for the FBI

(U) When a subject's fingerprints are submitted by another criminal justice agency for the FBI, the FBI FO must be listed as the contributor, along with the date of arrest, charge, and descriptive data. The submitted fingerprints may be submitted with a request to copy/reply to a

local criminal justice agency, if interested, as indicated in the EBTS available at [redacted] b7E

4.1.11. (U) Types of Fingerprint Cards

(U) Fingerprint cards are distributed free of charge to criminal justice agencies. CJIS recommends that fingerprint submissions be transmitted electronically; however, the fingerprint cards listed below are available.

4.1.11.1. (U) "Criminal Fingerprint" Card (FD-249)

(U) The FD-249 "Criminal Fingerprint" card is used by criminal justice agencies to record the fingerprint impressions of those persons who have been arrested or incarcerated in penal institutions. A criminal card includes information regarding the arrest charge, the disposition, and other information relating to the physical description of the arrested or incarcerated individual. Space is provided for the UCN, which must be indicated when known. Spaces are also provided for the contributor of the fingerprints to indicate whether a reply is desired. Due to the requirements of CJIS's NGI, when a contributor places a UCN on the fingerprint card, it is also necessary to submit a full set of fingerprints.

4.1.11.2. (U) "Applicant" Fingerprint Card (FD-258)

(U) The FD-258 fingerprint card is used to submit fingerprints to CJIS for persons directly employed in, or applying for, criminal justice positions or in those instances where authorized by federal statute, Presidential EO, state statute pursuant to Pub. L. 92-544, or regulation of the AG of the United States. An FBI applicant fingerprint card must be submitted with an electronic communication (EC) addressed to CJIS.

4.1.11.3. (U) "Personal Identification" Card (FD-353)

(U) The FD-353 "Personal Identification" card is used solely for recording the fingerprint impressions of those persons who voluntarily submit their fingerprints for purposes of identification only. These cards are available to anyone who chooses to forward his or her fingerprints to CJIS for retention. Personal identification fingerprint cards are maintained in the CJIS Division's NGI.

(U) With regard to a child's fingerprints that have been printed by parents for identification purposes, the parents are urged to retain the child's prints, which should be forwarded to the appropriate law enforcement authorities only if the child goes missing.

4.1.11.4. (U) Major Case Fingerprint Cards (FD-249, FD-884, and FD-884a)

(U) For major case prints, three different forms are used to capture a complete set of friction ridge impressions on an individual's hands. The FD-249 ("Criminal Fingerprint") is used to capture an individual's fingerprints in the form of rolled and flat impressions. The FD-884 ("Palm Print") is used to capture various impressions from the palmar surface of the hand, specifically the underside of the hand or palmar area, the little finger edge of the hand, and the rolled finger impressions of the hand. The FD-884a ("Supplemental Finger and Palm Print") is used to capture additional friction ridge details present on the hand, specifically the details

present on the extreme sides and tips of the fingers and thumbs, and the friction ridge details present in the thenar area (flesh at the base of the thumb) of the palm.

4.1.11.5. (U) Fingerprint Cards not Distributed by the FBI but Processed in the Criminal Justice Information Services Division

4.1.11.6. (U) [redacted] b7E

(U) [redacted]

4.1.11.7. (U) Armed Forces Fingerprint Card (DD-2280)

(U) The DD-2280 fingerprint card is used by the U.S. Air Force, Army, Coast Guard, Marine Corps, and Navy to record the fingerprints of military personnel.

4.1.11.8. (U) Note Concerning the Alien Registration Fingerprint Card (AR-4)

(U) The AR-4 fingerprint card was used by the U.S. Department of State and the United States Immigration and Naturalization Service (INS) (now known as the United States Citizenship and Immigration Services [USCIS]). CJIS has filed these fingerprint cards since 1940 when the Alien Registration Act (concerning the fingerprinting of aliens) went into effect. The fingerprinting requirement in the act was rescinded in 1986; therefore, such cards are no longer being received for filing.

4.1.12. (U) Files in the Criminal Justice Information Services Division

4.1.12.1. (U) Master Criminal Fingerprint File

4.1.12.1.1. (U) Retained Fingerprint Submissions

(U) The first "criminal retain fingerprint" submissions received for persons arrested or incarcerated by local, state, tribal, and/or federal authorities are assigned a UCN. These images are stored electronically in the Advanced Fingerprint Identification Technology segment of the NGI. When a subsequent set of retain fingerprints is submitted and identified through fingerprint comparison with the first arrest of an individual in CJIS's NGI, the images may be updated with any superior images and/or any changes to the fingerprints, such as scars, amputations, and the like. If the record has not been fully automated by this point, the record will be fully automated before the processing of the "criminal retain fingerprint" submission is complete. All wanted, flash, and missing persons notices are placed in a subject's computerized criminal name record. In addition to persons arrested or incarcerated, unidentified missing persons and unknown deceased fingerprint submissions are also retained.

4.1.12.1.2. (U) Criminal Subject Search

(U) The name and descriptive information (e.g., sex, race, DOB, place of birth, SSN, and aliases) appearing on a criminal fingerprint submission submitted to CJIS will be indexed in the III search.

4.1.12.1.3. (U) Manual Civil Fingerprint File

(U) "Civil retain prints" received by CJIS are stored electronically. Civil submissions are received electronically from local, state, tribal, and federal agencies for federal employment, military service, alien registration and naturalization, personal identification, and other legislatively authorized purposes. The electronic prints are transmitted through CJIS's WAN or Shared Enterprise Network (SEN) to the FBI. Electronic submissions are imported into the NGI for processing.

4.1.12.1.4. (U) Civil Names Indices

(U) Names of military personnel, federal employees, aliens, and miscellaneous applicant-type fingerprints appearing on fingerprint cards, as well as fingerprints submitted for personal identification, are indexed on 3-inch by 5-inch cards. The name, race, height, weight, DOB, registry number (e.g., military service and alien registration numbers), submitting agency, Henry Classification, and UCN of an individual, if known, appear on this card. The 3-inch by 5-inch cards have been automated and divided into a male and female file for electronic search capability. The manual Civil Name Index is no longer maintained at CJIS.

4.1.12.2. (U) Missing Person Fingerprint File

(U) The fingerprint card for a person reported as missing is kept in CJIS's Master Criminal Fingerprint File until CJIS is advised by the contributor to remove the card or until the person reaches the "maximum retention age." This file contains fingerprint cards of persons reported as missing to law enforcement agencies and have been entered into the National Crime Information Center (NCIC) Missing Person File under any of the NCIC entry criteria. The criteria are set forth in the *NCIC 2000 Operating Manual*.

4.1.12.3. (U) Universal Control Number

(U) Each criminal fingerprint submission retained in CJIS Division files is given a UCN if one has not been assigned previously. A number is assigned upon receipt of an individual's first set of fingerprints. UCNs are assigned in numerical sequence, and no distinction is made between males and females. Assignment of a UCN does not mean that an individual has an arrest record, since certain civil fingerprint submissions are also assigned UCNs. When a UCN is known for an individual, it must be referred to in correspondences. A UCN will be found:

1. (U) In CJIS's NGI.
2. (U) On a "master" fingerprint card in CJIS's manual fingerprint card file.
3. (U) On other fingerprint cards in folders called "jackets" that also contain a variety of CHRI for an individual.
4. (U) On fingerprint cards/microfilm records.

4.1.12.4. (U) Dead File

(U) CJIS deactivates a CHR only when a current fingerprint(s) submission taken from a deceased person is matched to a record or if a Fingerprint Identification Indicator submission is received from a state in conjunction with the NFF. The fingerprint card of an unidentified deceased person

sent from a state identification bureau to CJIS as "John Doe," "Jane Doe," or "Unknown" will be searched in the criminal and civil fingerprint files. If no identification is made, the fingerprint image will be retained for a period of seven years and then destroyed.

(U) Fingerprint submissions for deceased persons whose identities are known will be processed and the record deactivated. CJIS will accept and process all fingerprint images of known deceased persons if the images are accompanied by correspondence or notations on the actual fingerprint cards, seeking positive verification of entitlement to veteran's benefits.

4.1.13. (U) Processing of Fingerprint Submissions at the Criminal Justice Information Services Division

(U) Fingerprint submissions received at CJIS demand prompt replies. Received fingerprint submissions are handled on a priority basis that is consistent with the urgency of each particular case. Generally speaking, arrest-type fingerprints from criminal justice agencies are given top priority, followed by various categories of applicant-type fingerprints. Electronic criminal submissions have [redacted] response time and electronic civil submissions have [redacted] response time. b7E

(U) On occasion, an emergency will arise, and a fingerprint submission will be submitted directly to CJIS's Special Processing Center (SPC) via fax or overnight express mail for an immediate search of the NGI. The SPC staff will honor such a request and process the fingerprint submission when the submission includes a letter on agency letterhead explaining the reason for the request. For any fax or overnight express mail submission indicating it as an emergency but not containing the requisite sending agency letter, SPC staff must contact the agency to convey this policy requirement in order to process the submission as an emergency and ensure that the requestor is authorized to receive the information.

(U) If the SPC staff received the request via fax, the staff will maintain all associated documentation for 30 days before it is destroyed. If the SPC staff receives a hard copy of the submission, CJIS will return the fingerprint submission to the submitting agency.

(U) Regardless of how the agency submitted the fingerprints to CJIS, the SPC staff will process the submission as a criminal inquiry that searches the NGI to determine if a criminal history exists for the subject. CJIS will not maintain the arrest data on the submission. If the arresting agency wants CJIS to maintain the arrest data on the fingerprint submission, the agency must resubmit the fingerprints electronically for assignment of a UCN to the submission or to update an existing record. When the agency resubmits the fingerprint submission electronically, CJIS staff will update the individual's criminal history report and forward a copy of the report to the agency.

(U) Only the most urgent requests for criminal history checks should go through the SPC via fax or by other expedited means. All other requests must be submitted electronically.

(U) Agencies with questions should contact the SPC by telephone at (304) 625-5584 or by fax at (304) 625-5587.

4.1.13.1. (U) Requirements to Obtain Criminal History Record Information

(U) In order to obtain CHRI, one of the following must be submitted:

1. (U) Fingerprints for comparison.
2. (U) An individual's name, plus UCN or FBI number. The III should be accessed initially to determine if an arrest record is available through the III before an inquiry is made of CJIS.

(U) For additional assistance, contact the Customer Service Group at 304-625-5590.

4.1.13.2. (U) Procedures for Requesting Records for Field Offices

4.1.13.2.1. (U) b7E

4.1.13.2.2. (U) Requests for Photographic Copies of Fingerprint Images by FBI Field Offices

(U) FBI FOs requesting photographic copies of fingerprint images must adhere to the following procedures:

1. (U) Draft an EC or send a fax to FBIHQ, CJIS Division, Attention: BSS.
2. (U) Include the UCN and indicate the number of copies needed in the request.
3. (U) If the subject is a fugitive, the office of origin (OO) must ensure that the fugitive's UCN is entered in his or her Wanted Person File record in NCIC before requesting copies of the fingerprint images.

4. (U) Request electronic copies of fingerprint images via the Fingerprint Image Request. This transaction enables electronic users to retrieve ten-print images from the FBI Criminal Tenprint FIMF.

4.1.14. (U) Certification of Identification Records and Fingerprints

(U) The AD or one of the deputy assistant directors (DAD) at CJIS will certify identification records upon issuance of a court order requiring certification. These records are typed with or without abbreviations, as long as they are used consistently throughout the document, and the certification is in accordance with 28 U.S.C. § 1733. Fingerprints can also be certified under the same citation. Requests for certifications should be limited to court cases or other special situations requiring the production of such records.

4.1.15. (U) Removing the Administrative Burden for Dispositions

(U) The CJIS Division will remove the administrative burden from all FBI FOs regarding dispositions. In collaboration with the United States courts and the United States Attorney's Office (USAO), the CJIS Division will either receive or research disposition information pertaining to federal convictions and federal nonconvictions. Therefore, it is no longer required for any FBI FO to submit disposition information to the CJIS Division. Although not required, an FO may continue to submit disposition information to the CJIS Division using its current processes.

4.1.15.1. (U) R-84 "Final Disposition Report" Form

4.1.15.2. (U) Use of the R-84 by Field Offices

- (U) The R-84 is used to report final dispositions of criminal cases in which fingerprints have been previously submitted to, and retained by, CJIS.
- (U) The form serves as a follow-up to a specific arrest.
- (U) Only one disposition form may be used to record the dispositions against any one individual.
- (U) If the FO chooses to send disposition information to the CJIS Division, only the original form needs to be sent; no fingerprints should be submitted.
- (U) If the FO chooses to complete an R-84, one copy must be retained in the FO file.

4.1.15.2.1. (U) Situations in Which to Not Use the R-84 Form

- (U) If the final disposition is known at the time fingerprints are submitted to CJIS, the disposition data must be submitted with the electronic submission of fingerprints, eliminating the need for the R-84.
- (U) If a subject has not been fingerprinted, there is no arrest record against which disposition data can be posted.
- (U) If the fingerprint submission was returned by CJIS for any reason (e.g., unclassifiable), and the fingerprints were not resubmitted by the contributor.

- (U) If reporting new arrest information, since arrest information must be furnished with the electronic submission of fingerprints.

4.1.15.2.2. (U) Data for Preparing the R-84 "Final Disposition Report" (Disposition Form)

(U) Disposition information can be sent to the CJIS Division using the various methods set forth in the Disposition Information Sheet.

4.1.15.2.3. (U) Return of the R-84 Form to the Contributor

(U) A disposition form must include sufficient information to allow CJIS to handle it without referring to previous submissions. If the required information is not furnished, or if no fingerprints for the offense are on file in CJIS's Criminal File, the disposition form must be returned to the contributor with the reason(s) for the return indicated.

4.1.15.2.4. (U) Accountability for Dispositions

(U) All missing dispositions on identification records received by personnel in the field must be accounted for. [redacted] b7E

[redacted]

4.1.15.3. (U) Data for Preparing an FD-65 "Fugitive Form Letter"

When completing an FD-65 "Fugitive Form Letter":

1. (U) Include the names of all fugitives involved in the case in the title appearing on the FD-65.
2. (U) Forward an EC, via Sentinel, to the attention of the Criminal Investigative Division (CID) immediately after the fugitive process is obtained.
3. (U) Do not delay the submission of the macro format while obtaining additional descriptive information that is not readily available.

4.1.15.3.1. (U) Data for Supplemental Submission

(U) Additional descriptive information pertinent to the original FD-65 "Fugitive Form Letter" may be provided subsequent to the initial submission.

1. (U) Mark the appropriate field of the macro format.
2. (U) Refer to the date of the initial submission.
3. (U) Insert either the new information or the word "delete" in the appropriate spaces on the form macro if the information previously furnished is no longer accurate.

4.1.15.3.2. (U) No Initial Submission

(U) An initial fugitive EC and an FD-65 are not necessary in cases involving paroled or mandatory-release violators or deserters; however, a supplemental FD-65 must be submitted to show any changes, additions, or deletions to identifying data.

4.1.15.3.3. (U) No Supplemental Submission

(U) It is not necessary to submit a supplemental form when a subject's UCN and fingerprint classification are furnished by CJIS; however, these items should be modified in the subject's NCIC Wanted Person File entry when a positive identification is indicated via the [redacted] form. b7E

4.1.15.3.4. (U) Results of Submission

(U) When the NCIC provides CJIS with warrant information that has been entered into the NCIC Wanted Person File, the wanted notice on any federal fugitive is routinely placed in CJIS's criminal record file or in the automated name indices if no record exists.

(U) Arrest and disposition data for all fugitive matters must be forwarded promptly to CJIS. Any photograph(s) of a fugitive should be provided to CJIS.

1. (U) Six months after an individual has been declared a fugitive, the OO must review its files to determine the desirability of requesting background data from CJIS. The assistant director in charge (ADIC) or SAC of an individual FO must personally approve each such request. If it is believed that background information in a subject's identification record might cause prompt apprehension, a request may be made at any time, provided that the ADIC/SAC personally approves the request.
2. (U) Background data furnished from the subject's identification record should be forwarded to the appropriate case agent or designee, the pertinent portion of which should be included in the next investigative report. Descriptive data furnished by CJIS may be duplicated for inclusion in the investigative report. These instructions do not alter the policy of quoting the complete identification record of all subjects in an investigative report.

4.1.15.4. (U) Determining a Fugitive's Universal Control Number as a Means of Positive Identification

(U) If an FO is unable to locate an identification record that is a match with a fugitive through the III inquiry, an EC must be forwarded to CJIS, Attention: Answer Hits to Wants Team, and it should include any available fingerprints of the fugitive so that a technical fingerprint search can be conducted and a positive stop based upon fingerprints can be placed. A fingerprint-based stop means that incoming applicant/criminal fingerprint cards in alias names will hit against the stop, thereby triggering notification(s) to the appropriate FO.

4.1.15.5. (U) "Criminal Justice Agency Wanted-Flash-Cancellation Notice" (1-12)

(U) This form is available to all local, state, tribal, and federal criminal justice agencies. It is not to be used by FBI FOs.

4.1.15.5.1. (U) Information for Preparing a 1-12 Notice

(U) A 1-12 notice should be filled in completely so that the identification record for the subject can be located. The UCN must be given, if known. If not known, fingerprints must be submitted.

4.1.16. (U) Acknowledgement of Fingerprints by the Criminal Justice Information Services Division

(U) All fingerprint submissions containing information about offenses will be searched automatically against the NGI. Any nonoffense, such as an inquiry or question of identity, will not be retained; however, a positive or negative response will be returned to the fingerprint contributor.

4.1.16.1. (U) Submitted Fingerprints Identical with a Prior Record (an "Ident")

(U) When a search of the identification files locates a prior record, the received fingerprint submission is acknowledged by an FBI identification record that sets forth, in detail, the fingerprint record available on the individual and furnishes a UCN that should be referenced in all subsequent communications. Copies needed for other agencies must be indicated by the contributor on the fingerprint submission and not in a cover EC. Requests for additional copies should be kept to a minimum.

4.1.16.2. (U) Submitted Fingerprints Not Identical with a Prior Record (a "Non-Ident")

(U) When a search fails to reveal prior arrest data, a non-ident-response that reads, "A search of the fingerprints on the above individual has revealed no prior arrest data," is returned to the contributor of the fingerprints.

4.1.16.3. (U) Fingerprints Submitted by Local, State, Tribal, and Federal Criminal Justice Agencies

4.1.16.3.1. (U) Multiple Submissions

(U) Special agents (SA) in daily contact with local, state, tribal, and federal criminal justice agencies must remain alert to detect instances of multiple fingerprinting of the same individual by two or more agencies on the same or a related offense. Such due diligence avoids duplicative efforts and ensures the most efficient use of CJIS staff. This may be accomplished by a notation on the fingerprint submission, requesting additional copies of record(s) for agencies that might otherwise fingerprint the individual for the offense.

4.1.16.4. (U) Mail and Wire Service

4.1.16.4.1. (U) First-Class Mail

(U) Written acknowledgments to requests received in CJIS are sent by first-class mail. However, if the request is from the FBI or an agency that provided its Federal Express account number, the acknowledgement will be sent via Federal Express.

4.1.16.4.2. (U) Wanted Wires

(U) Wanted wires are sent via the International Justice and Public Safety Information Sharing Network when NCIC originating agency identifiers are available.

4.1.16.4.3. (U) Not Forwarded Automatically

(U) Current copies of arrest records are not forwarded automatically to agencies that had previously submitted fingerprints unless the agencies have posted wanted or flash notices against records.

4.1.17. (U) Expungement of Fingerprints by the Criminal Justice Information Services Division

4.1.17.1. (U) Fingerprints Submitted by Federal Criminal Justice Agencies

(U) The United States Department of Justice (DOJ) has advised that arrest fingerprints taken by a federal agency or by a nonfederal agency at the request of a federal agency are official USG records. As such, they cannot be destroyed, except upon the issuance of a federal court order. United States attorneys (USA) have been instructed to vigorously oppose motions to expunge federal CHRs unless a USA is convinced that the interest of justice requires that a record be expunged. For example, expunction may be appropriate when an arrest is based upon a case of mistaken identity. Complete instructions pertaining to requests for expungements (fingerprints and photographs) relating to federal cases are found in DOJ Memorandum Number 765 to all U.S. attorneys, dated March 6, 1972, captioned "Motion for Discovery, or Expungement of, Arrest Records Held by the FBI."

4.1.18. (U) Foreign Fingerprints Exchange

(U) The Global Initiatives Unit (GIU) is the primary POC for CJIS's Foreign Fingerprint Exchange. Principal among the GIU's goals is the development of international, bilateral agreements to exchange fingerprint data. Working with interagency partners, GIU personnel have acquired over one million fingerprint records. These records reside within the FBI NGI and represent a portion of the FBI's growing fingerprint-based contribution to DHS and DoD counterterrorism efforts. Fingerprints are obtained via exchange efforts through technical solutions, as well as during foreign travel by FBI personnel.

4.1.18.1. (U) Request for Foreign Search

(U) The requesting FO or legal attaché (Legat) office must contac[redacted] within CJIS to coordinate a search of a foreign partner fingerprint repository or system. [redacted] number is [redacted] (24 hours a day, seven days a week). b7E

4.1.19. (U) FBI Literature Concerning Criminal Justice Information Services Division Work and Functions

(U) The TRTT at CJIS provides training and expert witness testimony in the science of fingerprints, including all the proper preparation and processing of friction ridge skin and CHR data to agencies with authorized access to CJIS systems. The TRTT offers a variety of classes conducted at CJIS in Clarksburg, West Virginia. In addition, some courses are available via video teleconferencing. Agencies are encouraged to send their employees to CJIS for fingerprint and criminal history training from the TRTT. These internal classes are scheduled on a quarterly basis and are advertised on the FBI's Internet site at <www.fbi.gov>.

4.1.20. (U) Requests for Copies of Fingerprint Cards

(U) To request copies of fingerprints on file, call (304) 625-5584, or direct written requests to CJIS, BSS, Special Processing Center, Clarksburg, West Virginia.

4.2. (U) Latent Fingerprint Identification

4.2.1. (U) Laboratory Division: Latent Print Units and Programs

(U) The mission of the LD is to apply scientific capabilities and technical services for the collection, processing, and exploitation of evidence for the FBI and other duly constituted law enforcement agencies in support of investigative and intelligence priorities. The LD conducts analyses on physical evidence ranging from blood and other biological materials to explosives, drugs, and firearms and conducts research and development for new forensic technologies and techniques. Laboratory examiners provide expert-witness testimony in court cases regarding the results of forensic examinations, and specially trained teams assist domestic and international law enforcement agencies with large-scale investigations and disaster response, including weapons of mass destruction response support and crime-scene documentation. The LD also coordinates and manages the unified efforts of intelligence and military assets to technically and forensically prevent potential improvised explosive device (IED) attacks.

(U) The Latent Print Units consist of the Latent Print Operations Unit (LPOU) and the Latent Print Support Unit (LPSU).

4.2.1.1. (U) The Latent Print Operations Unit

(U) LPOU's mission is to conduct timely, high-quality scientific examinations in the area of friction ridge analysis. The LPOU examines, processes, preserves, and compares friction ridge impressions; documents the results of examinations in case notes and official reports; and testifies to results in legal proceedings. Examiners conduct crime scene examinations, attempt to identify victims of mass fatalities, and provide training. This unit also provides technical assistance regarding friction ridge matters to the law enforcement community worldwide.

(U) LPOU conducts all work on evidence submitted to the LD pertaining to the development and comparison of latent fingerprints, palm prints, and footprints. In special circumstances, such as when an item is too large or when the volume is too great to be mailed, LPOU forensic examiners respond to crime scenes to conduct latent print examinations. In unknown-subject cases or in cases where no identifications have been made, LPOU conducts computerized searches of latent prints in the FBI's automated database. The examination of fingers and hands of unknown deceased individuals is handled in LPOU by examiners who use special techniques in their attempts to identify unknown individuals. LPOU forensic examiners form the nucleus of the FBI Disaster Squad, which assists in the identification of victims of mass fatality incidents. LPOU forensic examiners testify to the results of their examinations in county, municipal, state, tribal, federal, military, and foreign courts. LPOU forensic examiners have the ability to provide training to local, state, tribal, federal, and foreign law enforcement personnel in all aspects of friction ridge analysis.

4.2.1.2. (U) Latent Print Support Unit

(U) LPSU's mission is to provide oversight and management of various friction ridge analysis programs and initiatives. These include the latent aspects of the Next Generation Identification Program, the Major Incident Management Program, the Research Program, the Standards and Practices Program, the Technology Development Program, the Training Program, and forensic systems. LPSU also prepares technical correspondence and articles for publication and provides technical assistance regarding friction ridge analysis matters to the law enforcement community worldwide.

4.2.1.2.1. (U) Next Generation Identification Program

(U) The NGI program provides procedures for using the FBI's automated database to ensure accurate, reliable search results and to coordinate, test, evaluate, and implement new NGI software. The NGI program also provides liaison with CJIS and the criminal justice community on latent print-related NGI issues, supports NGI development and the replacement and maintenance of NGI hardware, and coordinates with system administrators to resolve NGI problems.

4.2.1.2.2. (U) Major Incident Management Program

(U) The Major Incident Management Program coordinates the operational response of personnel in the LPU, which includes managing and maintaining the infrastructure for the FBI Disaster Squad and the latent component of FBI Hazardous Evidence Analysis Team (HEAT), serving as the POC for deceased processing and associated ante mortem/post mortem record requests, and providing worldwide technical, educational, and research support for disaster victim identification issues.

4.2.1.2.3. (U) Research Program

(U) The Research Program develops and applies optimal science and technology through internal and external research and development projects; manages, coordinates, and directs all research projects related to the science of friction ridge analysis; and acts as the POC for all latent print-related research issues that arise in the discipline.

4.2.1.2.4. (U) Standards and Practices Program

(U) The Standards and Practices Program ensures that the LPU maintains accreditation and conducts high-quality work. Activities include drafting, implementing, and maintaining the *Latent Print Operations* and *Quality Assurance* manuals; managing corrective and preventive actions; and coordinating the LPU portions of internal and external audits. This program also acts as the POC for questions regarding the quality system of the LPU and quality document requests.

4.2.1.2.5. (U) Technology Development Program

(U) The Technology Development Program coordinates, tests, evaluates, and implements relevant biometric and digital imaging technology; liaises with the criminal justice community on all biometric and digital imaging issues; coordinates and manages the operation of the Latent Print Digital Imaging System (LPDIS); provides procedures for the use of LPDIS to obtain the

best possible friction ridge/friction ridge print images; and coordinates, tests, evaluates, and implements new LPDIS software.

4.2.1.2.6. (U) Training Program

(U) The Training Program manages, coordinates, and directs the training programs for the Latent Print Units, including physical scientist/forensic examiner training; recruits new potential examiners; reviews transcripts to ensure continuing education opportunities for examiners; develops curriculum for training provided by qualified examiners; recruits potential examiners; and makes recommendations for conference presentations and attendance.

4.2.2. (U) Procedures and Processes of the Laboratory Division's Latent Print Units

4.2.2.1. (U) Automated Searching of Latent Fingerprints

(U) The NGI provides the LPOU with several capabilities to conduct computer-based latent print searches against known print repositories. NGI includes the capability to search an unidentified latent print against the FBI's files, and share information with other NGI databases through coordinated efforts with CJIS and LFSU.

(U) The ability to conduct NGI latent print searches is a capability that may result in identifications and the solving of crimes that would otherwise remain unsolved; however, the traditional practice of developing and naming suspects/subjects from the investigative process, along with the acquisition of fingerprints from victims and others, must still be followed. When communicating with the LPOU, NGI searches must be specifically requested. The LPOU forensic examiner will assess each case and, based on the information provided, initiate appropriate searches.

4.2.2.2. (U) Latent Print Examinations

4.2.2.2.1. (U//~~FOUO~~) Use of the Technical Expertise of the FBI's Latent Print Unit in the Examination of Evidentiary Materials – Bureau Cases, State and/or Local Facilities

(U//~~FOUO~~) Materials of evidentiary value located at crime scenes or otherwise obtained during investigative activities offer invaluable potential for investigative information and probative results; moreover, the database of persons represented in the known print files of CJIS is far greater than that available to local and/or state authorities. For these reasons, LPOU should be contacted in FBI cases requiring latent print examinations.

4.2.2.2.1.1. (U//~~FOUO~~) Joint Jurisdiction

(U//~~FOUO~~) Processing or comparisons done by a local or state laboratory due to extenuating circumstances, such as preexisting forensic involvement with crime labs at the local or state level, may prohibit any future involvement of the LPOU. In many cases, the LPOU will perform processes or use alternate light sources that may not be available at the local or state level. Many of these examinations cannot be conducted after a local or state lab has processed an item. Additionally, the LPOU will not repeat or perform comparisons and examinations already performed by a local or state examiner without the approval of the AD, LD.

4.2.2.2.1.2. (U//~~FOUO~~) Conditions for Use of State or Local Facilities

(U//~~FOUO~~) When circumstances and good judgment dictate that consideration be given to using local or state fingerprint technicians and/or crime laboratory personnel in FBI cases, the following conditions must be met before a decision is made:

1. (U//~~FOUO~~) The SAC must be fully aware of the facts of the case and the nature of the examination(s) to be conducted. Whether or not the local or state laboratory will perform all of the techniques available to the LPOU should be taken into consideration, and it should be noted that the LPOU will not repeat or perform comparisons and examinations already performed by another local or state examiner without the approval of the AD, LD.
2. (U//~~FOUO~~) Extenuating circumstances, such as preexisting forensic involvement with crime labs at the local or state level, must exist that justify SAC approval for the use of local or state facilities and personnel.
3. (U//~~FOUO~~) It is necessary to use the correct processing techniques and sequences in order to avoid the destruction of latent prints and to increase the possibility of enhancing latent prints. Therefore, if possible, the LD's LPOU should be contacted before processing begins. This will help ensure that the proper techniques and sequences are used. Improper processing sequences may preclude the use of additional methods of processing.

(U) In cases where local examinations are conducted and additional support from the LPOU is requested, copies of local or state reports must be included with requests.

4.2.2.2.1.3. (U//~~FOUO~~) Searching for Latent Prints

(U//~~FOUO~~) The search for latent prints must be conducted in a systematic and intelligent manner. Articles bearing or suspected of bearing latent impressions must be handled with extreme care, as these impressions are extremely fragile, and even the slightest contact with another surface may destroy them. [redacted] b7E

[redacted]

(U//~~FOUO~~) [redacted]

[redacted]

Should that be impossible, the part of the article that will be handled must first be examined for latent impressions. The light from a strong flashlight or other high-intensity light source is helpful in locating latent prints, as light reflected at an angle often shows the presence of latent prints.

(U//~~FOUO~~) Latent prints must be searched for in the following instances:

1. (U//~~FOUO~~) Surfaces and articles that may have been handled by the criminal at the scene of the crime. Circumstances may warrant examining certain areas of a victim's body for latent prints left on the skin. [redacted] b7E
2. (U//~~FOUO~~) Property that was received under any circumstances and was also believed to have been stolen.
3. (U//~~FOUO~~) Vehicles, weapons, tools, and other articles that may have been used in the commission of a crime, even if they are recovered at a distance from the crime. When impressions have been caused by a substance that contrasts in color with the surface on which they were made, they will usually be visible, though they may not be conspicuous. Such impressions may result from a dirty, oily, or bloody hand coming into contact with a relatively clean surface. If the impressions have been made in plastic substances such as wax or clay, they will be visible and must not be further processed in any manner.

(U//~~FOUO~~) Any time a latent print is visible on an item or on a surface, it should be photographed by a trained latent photographer in a manner that complies with required LPOU standards (see subsections 4.2.2.6. and 4.2.3. of this PG) prior to any collecting, packaging, or additional processing of the item or surface.

4.2.2.3. (U//~~FOUO~~) Development of Latent Impressions

(U//~~FOUO~~) All evidence that is not too bulky and is portable must be submitted to the LPOU for latent print examination. Field support may be obtained by contacting the local FO's emergency response team (ERT) for the processing and/or collection of all evidence. (Note: See subsection 4.2.3. of this PG for more information on the submission of evidence.)

4.2.2.4. (U//~~FOUO~~) Developing, Photographing, and Lifting of Latent Prints

(U//~~FOUO~~) All visible latent prints must be photographed prior to further processing or being shipped to the LPOU. When a print is clearly visible on any surface, it should be photographed before attempting to further process the surface. Sometimes, due to poor contrasts, reflections of light, multicolored surfaces, or the physical location of a latent print, it may seem impossible to photograph the impression successfully; however, an attempt must be made to photograph all friction ridge detail observed. Photographs and negatives must include a scale or other measurable item if a search of the NGI is requested; however, photographs or negatives without a scale or other measurable item may be used for manual comparisons. See subsection 4.2.3. for additional requirements when submitting photographs, negatives, or digital images of latent print evidence.

4.2.2.5. (U//~~FOUO~~) Known Prints

(U//~~FOUO~~) The fingerprints and palm prints of all persons who have legitimately handled the articles must be taken for comparison with any latent prints. The prints of a deceased individual should be obtained before interment. SAs should be extremely careful in handling objects so as not to leave their own prints. If prints have been inadvertently handled, such information must be indicated in the transmittal letter. All fingerprints and palm prints submitted for comparison purposes must have the necessary descriptive data and the name of the individual whose prints

are recorded on each card. Signatures of the individual being printed, as well as the person taking the prints, must also appear on each card, along with the date the prints were recorded. If an individual refuses to sign, this refusal must be indicated on the card. Major case prints submitted for comparison purposes may be appropriately recorded on separate cards. Only one side of a card may be used to record fingerprints, palm prints, or major case prints. All fingerprints, palm prints, and major case prints intended for retention in CJIS files must bear narrative charges.

4.2.2.6. (U//~~FOUO~~) Submission of Evidence

4.2.2.6.1. (U//~~FOUO~~) Letters Submitting Evidence or Articles for Examination

(U//~~FOUO~~) An EC or FD-1121 "Laboratory Examination Request (LER)" form that requests latent print examinations must be drafted for any items submitted to the FBI Laboratory. This must be done every time an evidence submission is made, even if different submissions are part of the same investigation. The EC or LER must be directed to the Evidence Management Program, and packages must be addressed in the usual manner, marked "Attention: LD, Evidence Management Program." A sample LER for submitting evidence may be found on the [redacted] A copy of the EC or LER should be placed in the package. Letters transmitting evidence and requesting examinations must include a brief description of the evidence submitted, the circumstances of the investigation, and, if appropriate, the names of any individuals who should be compared in the case. Additionally, any priorities (e.g., trial dates) must be included, preferably in bold and at the beginning of the request. Fragile articles should be carefully packed and the package marked "Fragile." Labels designating the enclosure as "Evidence" must be placed on the inside wrappers. b7E

(U//~~FOUO~~) The Evidence Management Program must be contacted prior to the submission of any article or specimen that may have been contaminated by a person known to be infected with, or suspected of being infected with, acquired immune deficiency syndrome (AIDS), tuberculosis, or hepatitis in order to determine if the examination will be conducted. Any evidence that has been contaminated with blood or other bodily fluids must be clearly labeled "Biohazard."

4.2.2.7. (U) Latent Print Operation Unit Reports

Upon completion of the requested examinations, original latent print reports and the submitted evidence, if appropriate, will be furnished to the OO, unless otherwise directed.

4.2.2.8. (U) Submission of Photographs, Digital Media, and Negatives

(U) Photographs, digital media, and negatives of latent prints must include, if applicable:

1. (U) Documentation of the image source.
2. (U) Documentation of the capture device (e.g., scanner, digital camera, or traditional photography).
3. (U) Documentation indicating that the image is an original capture. When an image is submitted to the LPOU, the contributor must indicate that the image is the original capture. [redacted] b7E
4. (U) File properties as follows:

- [redacted] b7E
- [redacted]
- [redacted]

4.2.2.9. (U//~~FOUO~~) Preservation of Specimens During Shipment

(U//~~FOUO~~) [redacted] b7E

[redacted]

(U//~~FOUO~~) [redacted]

[redacted] Requirements for the labeling, marking, and shipping of body parts, as well as any potentially biohazardous materials, must be determined by contacting the carrier.

4.2.3. (U) Secondary Evidence

(U) Secondary evidence will be generated in the LPOU for prints that must be preserved because the prints may not retain the same quality or be detectable on the item of evidence over time. LPOU secondary evidence will be returned to the contributor for each submission, as applicable. These returned images can be photographs, digital images, photographic-quality prints of digital images, direct recordings of unknown deceased prints, or lifts generated by the examiner(s). LPOU secondary evidence is usually returned to the contributor with the original evidence.

4.2.4. (U) Requesting Copies of Records (Discoveries)

(U) Discovery requests for copies of any official examinations or administrative records must be made in writing. The case record includes examination and administrative records pertinent to a submission. All requests must be forwarded to the original examiner, the LPOU, or the FBI Laboratory.

4.2.5. (U) Testimony

(U) Latent print examiners are qualified to provide expert witness testimony in state, federal, and military courts. FOs should advise the LD's LPOU of any pending matters involving any phase of latent print testimony as a best practice, as it is not a requirement.

4.2.6. (U) Services of the Disaster Squad

(U//~~FOUO~~) The FBI Disaster Squad assists in the forensic identification of decedents from major disasters or mass fatality incidents that occur around the globe. A request must be made for

Disaster Squad assistance, and it can come from many different sources, including the ranking government agency/law enforcement official having jurisdiction over a disaster scene, the medical examiner or coroner in charge of victim identification, or a foreign government through the U.S. Department of State. FBI Disaster Squad participation involves the identification of victims through friction ridge analysis (fingerprints, palm prints, and footprints) and often utilizes the Automated Fingerprint Identification System (AFIS) remotely to expedite forensic identification efforts. The fact that Disaster Squad assistance centers around friction ridge analysis must be clearly explained to the requesting official at the time of the request so that the requester understands the extent and limitations of FBI Disaster Squad services.

(U) Major disaster/mass fatality incident questions should be directed to the program manager for LPSU's Major Incident Program.

4.3. (U) Legal Information for Civil Fingerprint Checks

(U) Certain determinations, such as employment, security, licensing, and adoption, may be predicated on fingerprint-based checks. Fingerprints and other information contained on, and along with, the fingerprint form may be submitted to the requesting agency, the agency conducting the application investigation, and/or the FBI for comparing the submitted information to available records in order to identify other information that may be pertinent to the application. During the processing of the application, and for as long thereafter as may be relevant to the activity for which the application is being submitted, the FBI may disclose any potentially pertinent information to the requesting agency and/or to the agency conducting the investigation. The FBI may also retain the submitted information in the FBI's permanent collection of fingerprints and related information, where it will be subject to comparisons against other submissions received by the FBI. Depending on the nature of the application, the requesting agency and/or the agency conducting the application investigation may also retain the fingerprints and other submitted information for other authorized purposes of those agencies.

(U) Routine uses: The fingerprints and information reported to the FBI may be disclosed pursuant to the subject's consent and may also be disclosed by the FBI without that person's consent, as permitted by the Federal Privacy Act of 1974 (5 U.S.C. 552a(b)) and all applicable routine uses as may be published at any time in the *Federal Register*, including the routine uses for the FBI Fingerprint Identification Records System (Justice/FBI-009) and the FBI's Blanket Routine Uses (Justice/FBI-BRU). Routine uses include, but are not limited to, disclosures to:

- (U) Appropriate governmental authorities responsible for civil or criminal law enforcement.
- (U) Counterintelligence, national security, or public safety matters to which the information may be relevant.
- (U) State and local governmental agencies and nongovernmental entities for application processing, as authorized by federal and state legislation, EO, or regulation, including employment, security, licensing, and adoption checks.
- (U) As otherwise authorized by law, treaty, EO, regulation, or other lawful authority.

(U) If other agencies are involved in processing an application, they may have additional routine uses.

(U) An applicant's SSN is needed to keep records accurate because other people may have the same name and DOB. Pursuant to the Federal Privacy Act of 1974 (5 U.S.C. § 552a), the requesting agency is responsible for informing the applicant whether disclosure is mandatory or voluntary, by what statutory or other authority an individual's SSN is solicited, and what uses will be made of it. EO 9397 also asks federal agencies to use this number to help identify individuals in agency records.

(U) The requesting agency and/or the agency conducting the application investigation should be able to provide an applicant with any additional information pertinent to the specific circumstances of his or her application, which may include identification of other authorities, purposes, uses, and consequences of not providing the requested information.

5. (U) Summary of Legal Authorities

(U) 28 U.S.C. § 534, 28 CFR § 0.85 (b) and (j), and §§ 20.1-20.38

(U) Appendix A: Sources of Additional Information

- (U) Departmental order information at <www.fbi.gov/checks>
- (U) Electronic Biometric Transmission Specification standards at [redacted] b7E
- (U) Universal Latent Workstation at [redacted]
- (U) CJIS Division form orders at <www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ordering-fingerprint-cards-and-training-aids>
- (U) "Guidelines for Capturing Palm Prints and Supplementals" at <www.fbi.gov>

(U) Appendix B: Contact Information

CJIS Division	**304-625-5590**
Biometric Services Section	Biometric Services Section CJIS Division 1000 Custer Hollow Road Clarksburg, WV 26306 [redacted] b7E
Biometric Center of Excellence	304-625-4555
Training and Records Testimony Team	[redacted]
Customer Service Group	304-625-5590
Latent Forensic Support Unit	[redacted]
Facial Analysis Comparison and Evaluation Services Unit	[redacted]

(U) Appendix C: Definitions and Acronyms

(U) Definitions:

(U) Biometric identification: Biometric identification consists of one or more methods used for recognizing humans based upon physical and/or behavioral traits that may be used to establish support of an individual's claimed identity or uniqueness (characteristics that clearly separate one individual person from other individual persons). Biometric characteristics fall into two main classes, physiological and behavioral. Physiological characteristics are related to the shape of the body.

(U) Acronyms:

ACS	Automated Case Support
AD	assistant director
ADIC	assistant director in charge
AG	Attorney General
AIDS	acquired immune deficiency syndrome
BCOE	Biometric Center of Excellence
BSS	Biometric Services Section
BSU	Biometric Support Unit
CAS	Civil Applicant System
CC	Compact Council
CFR	Code of Federal Regulations
CFTC	Commodity Futures Trading Commission
CHIPU	Criminal History Information and Policy Unit
CHR	criminal history record
CHRI	criminal history record information
CIA	Central Intelligence Agency
CID	Criminal Investigative Division

CJIS	Criminal Justice Information Services [Division]
CSPRO	Criminal Justice Information Services Security and Professional Responsibility Office
CSO	chief security officer
CSU	Customer Service Unit
DAD	deputy assistant director
DHS	Department of Homeland Security
DNA	deoxyribonucleic acid
DO	Departmental order
DOB	date of birth
DoD	Department of Defense
DOJ	Department of Justice
DOJCERT	Department of Justice Computer Emergency Response Team
DOT	Department of Transportation
EBTS	electronic biometric transmission specification
EC	electronic communication
ERT	emergency response team
EO	executive order
EOD	enter [entry] on duty
FBI-BRU	FBI blanket routine uses
FACE	Facial Analysis Comparison and Evaluation
FBI	Federal Bureau of Investigation

b7E

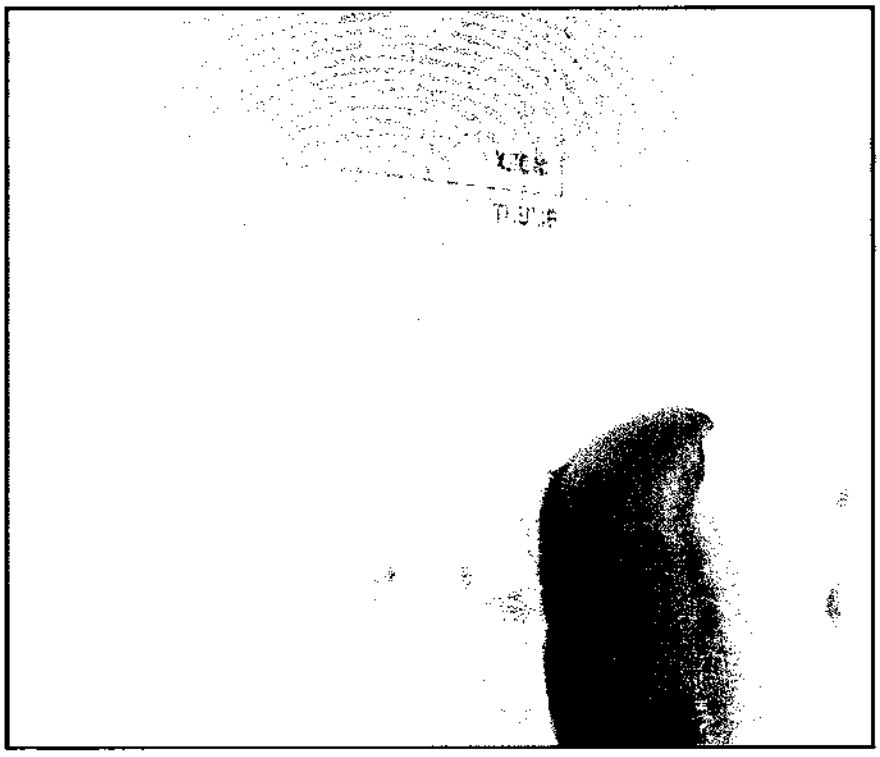
FBIHQ	Federal Bureau of Investigation Headquarters
FIMF	fingerprint image master file
FIP	Fingerprint Identification Program
FO	field office
GIU	Global Initiatives Unit
GOS	Global Operations Section
GSA	General Services Administration
HEAT	Hazardous Evidence Analysis Team
IAFIS	Integrated Automated Fingerprint Identification System
IdHS	identity history summary
IED	improvised explosive device
III	interstate identification index
INS	Immigration and Naturalization Service (now United States Citizenship and Immigration Services)
LD	Laboratory Division
LEEP	Law Enforcement Enterprise Portal
LER	Laboratory Examination Request [FD-1121]
Legat	legal attaché [office]
LFSU	Latent and Forensic Support Unit
LPDIS	latent print digital imaging system
LPOU	Latent Print Operations Unit
LPSU	Latent Print Support Unit
NARA	National Archives and Records Administration

NCIC	National Crime Information Center
NCMEC	National Center for Missing and Exploited Children
NCPPCC	National Crime Prevention and Privacy Compact Council
NFA	National Futures Association
NFF	national fingerprint file
NGI	Next Generation Identification
OGC	Office of the General Counsel
OO	office of origin
OPM	Office of Personnel Management
PG	policy guide
PII	personally identifiable information
POC	point of contact
Pub. L.	public law
QIU	Quality Improvement Unit
RFES	remote fingerprint editing software
SA	special agent
SAC	special agent in charge
SEC	Securities and Exchange Commission
SEN	Shared Enterprise Network
	b7E
SPC	Special Processing Center
SSN	social security number

STB	Science and Technology Branch
TRTT	Training and Records Testimony Team
TSA	Transportation Security Administration
UC	unit chief
UCN	universal control number
ULF	Unsolved Latent File
U.S.	United States
USA	United States attorney
USAO	United States Attorney's Office
U.S.C.	United States Code
USCIS	United States Citizenship and Immigration Services
USG	United States government
USPER	United States person (U.S. person)
WAN	wide area network

(U) Appendix D: Guidelines for Capturing Palm Prints and Supplementals

Guidelines for Capturing Palmprints and Supplementals

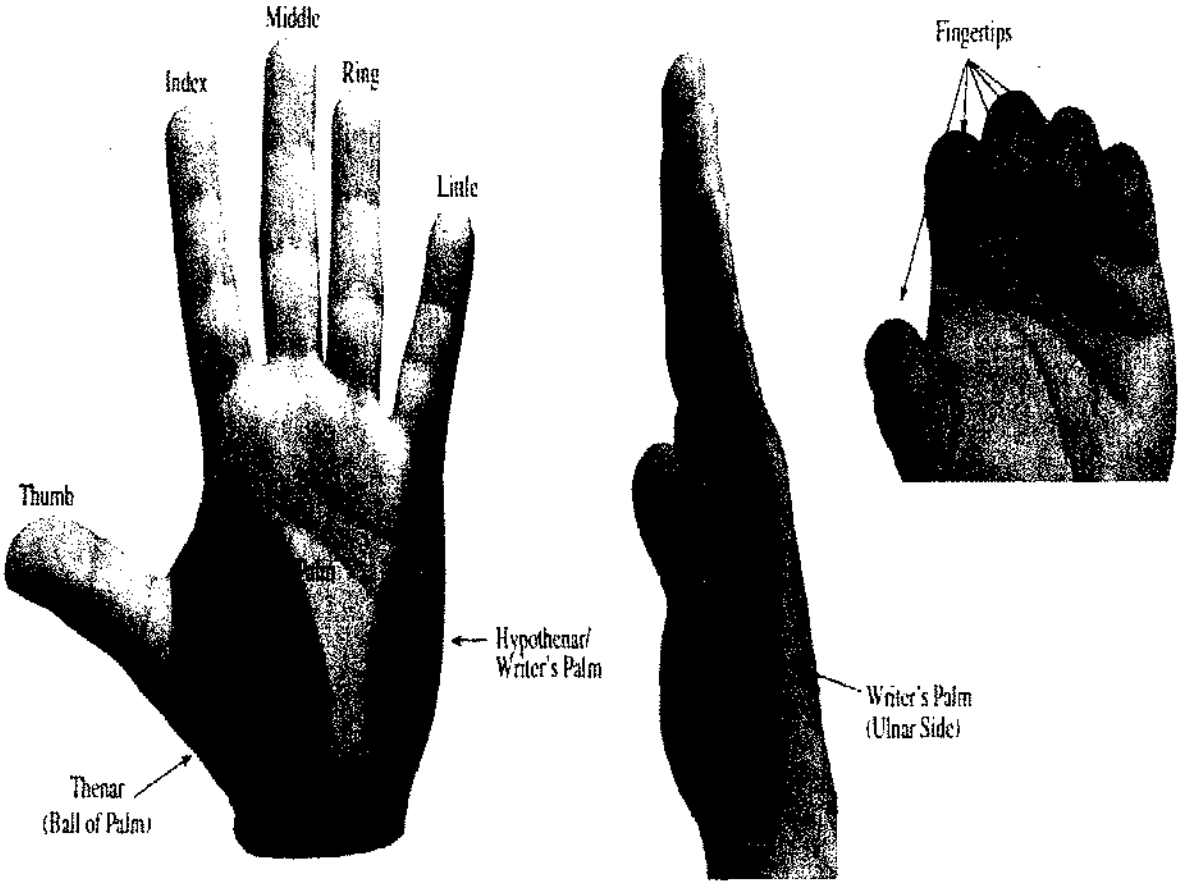


Guidelines for Capturing Palmprints and Supplementals

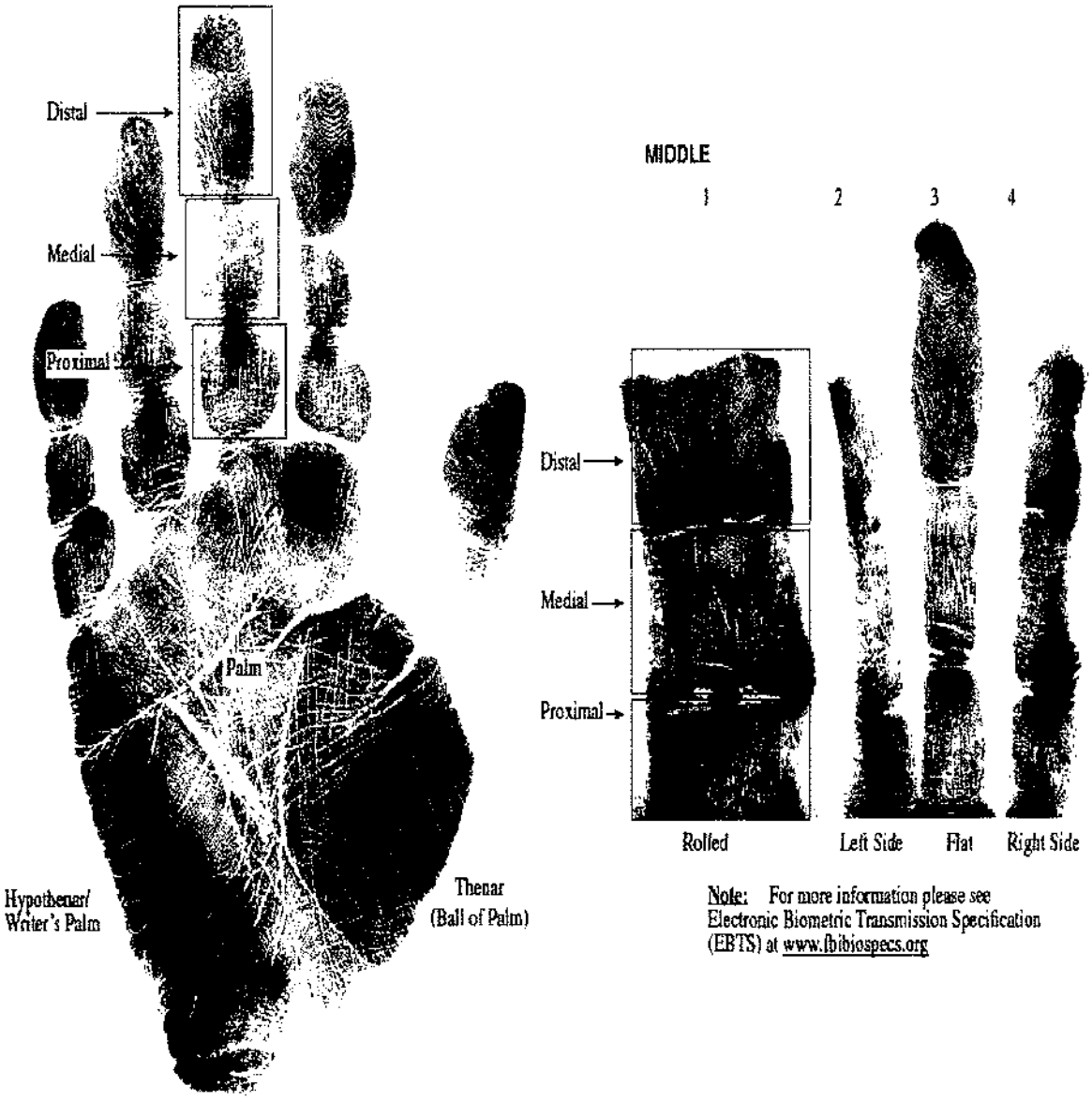
General Overview:

- The FBI will implement palmprint and supplemental print search capabilities as part of its Next Generation Identification (NGI) effort
- As of July 2010, the FD-884 (10-28-99) and FD-884a (5-07-07) have been revised and will be available in the near future. This guideline represents the final state, in which the only change made is the orientation of the text within the same capture block. Existing cards will be accepted; however, please ensure that the capture of the friction ridge information is oriented as depicted within this guide
- Orientation guidelines are provided for your reference

Hand with basic regions noted:



Hand with basic regions noted:



Note: For more information please see Electronic Biometric Transmission Specification (EBTS) at www.fbibiospecs.org

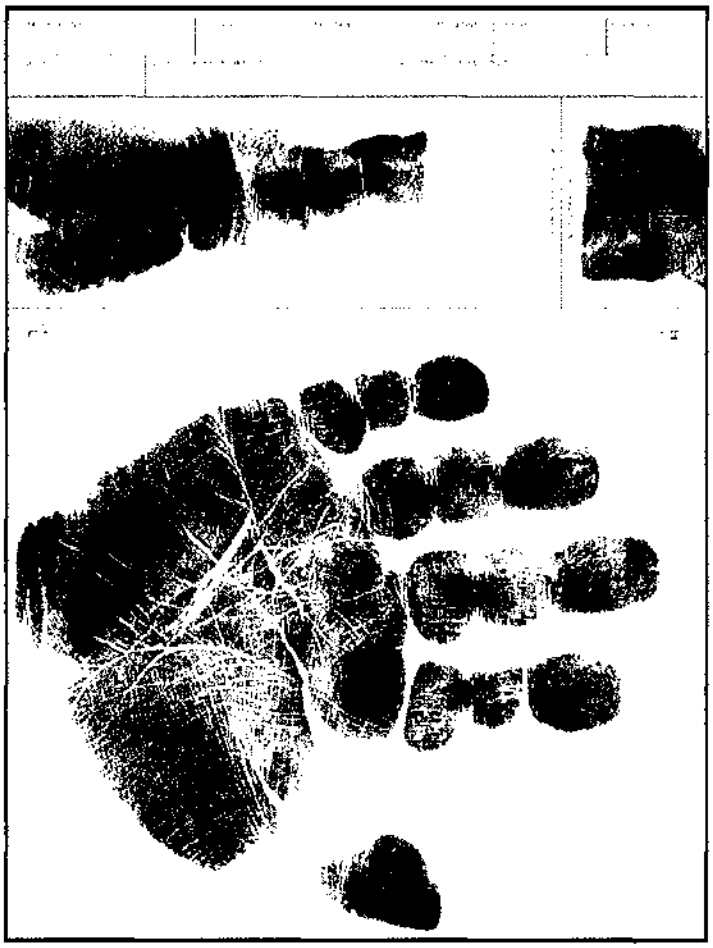
Form 884: Palmprint Card (Front Side)

This guide is for print orientation purposes only

- To ensure standard capture of each print, all fingers/tips/palms must be oriented in the direction of the text within the capture block
- Each impression must be captured completely within the box provided in a vertical, upright position

Writer's Palm Impression:
Ulnar side of hand placed in a vertical, upright position with base of wrist in line with edge of card and fingertip oriented in direction of text within the capture block.

Palm Impression:
Circle left or right palm orientation. Orientation of palm must mirror image of palm illustration in a vertical, upright position with base of wrist in line with edge of card and fingertips oriented in direction of image.



Index Finger:
Roll finger with tip oriented in direction of text within the capture block

Note:
Purpose is to verify palmprint with tenprint.

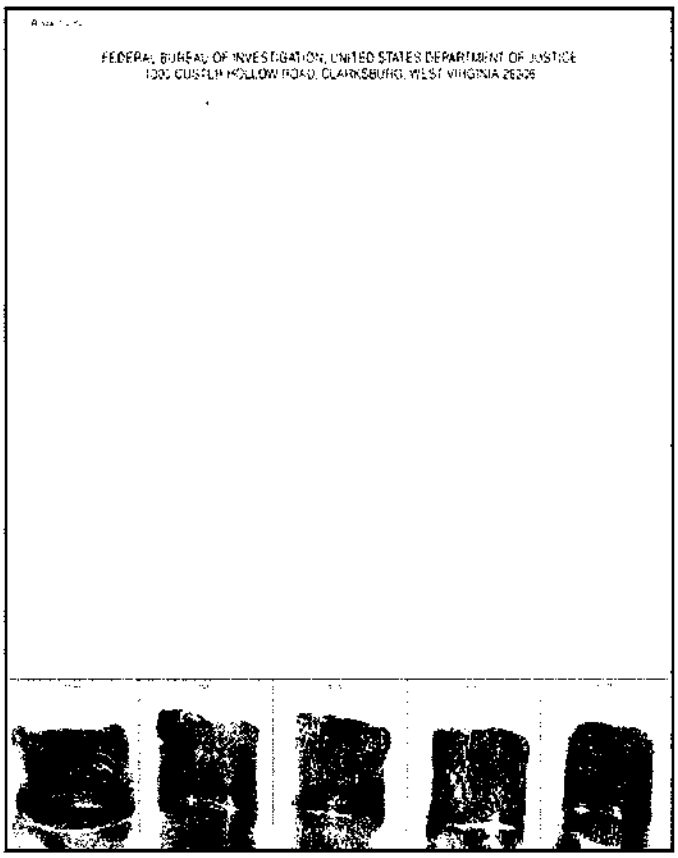
Form 884: Palmprint Card (Back Side)

- This guide is for print orientation purposes only.

Thumb Index Middle Ring Little

- Using the same hand printed on the front side of the card, roll each finger in the appropriate block.
- Each impression must be captured completely within the capture block provided in a vertical, upright position with fingertips oriented in the direction of text.

Note:
Area above rolled prints needs to remain blank.



Form 884a: Supplemental Finger and Palmprint Card (Front Side)

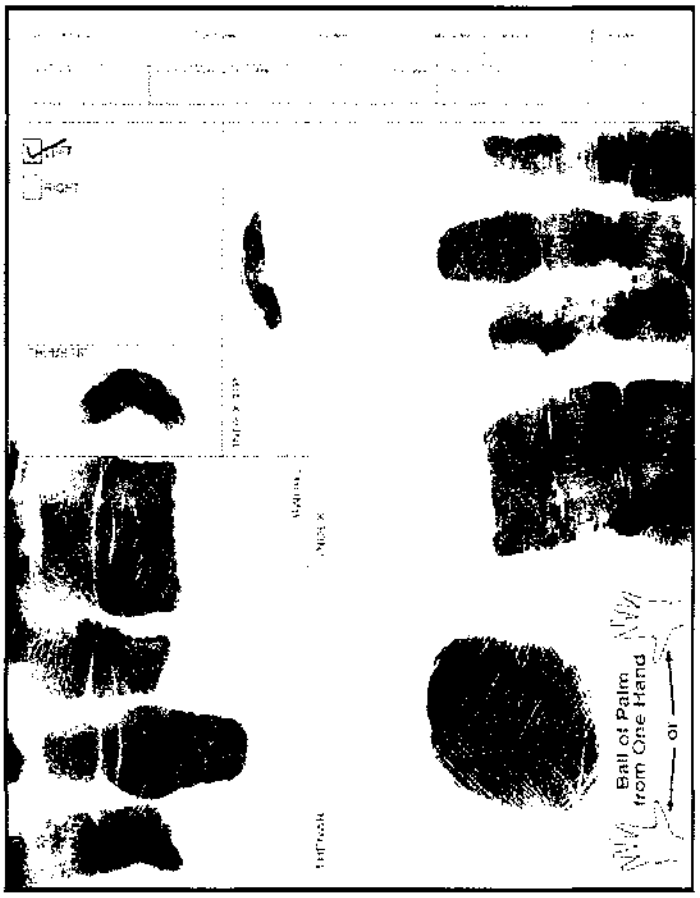
This guide is for print orientation purposes only

- To ensure standard capture of each print, all fingers/tips/palms must be oriented in the direction of the text within the capture block
- Each impression must be captured completely within the box provided in a vertical, upright position

Note:
Select Left or Right hand. Images must be captured in the following sequence: *fully rolled, left edge, flat, right edge* impressions.

Thumb Tip:
Orient tip of thumb in direction of text within the capture block.

Thumb:
Orient thumb in direction of text within the capture block.
Capture one *fully rolled* thumb impression.
Capture one *left edge* thumb impression.
Capture one *flat* thumb impression.
Capture one *right edge* thumb impression.



Index Tip:
Orient tip of index finger in direction of text within the capture block.

Index:
Orient index finger in direction of text within the capture block.
Capture one *fully rolled* index finger impression.
Capture one *left edge* index finger impression.
Capture one *flat* index finger impression.
Capture one *right edge* index finger impression.

Thenar:
Orient ball of palm in the direction of text within the capture block with base of wrist in line with edge of card. Obtain an impression.

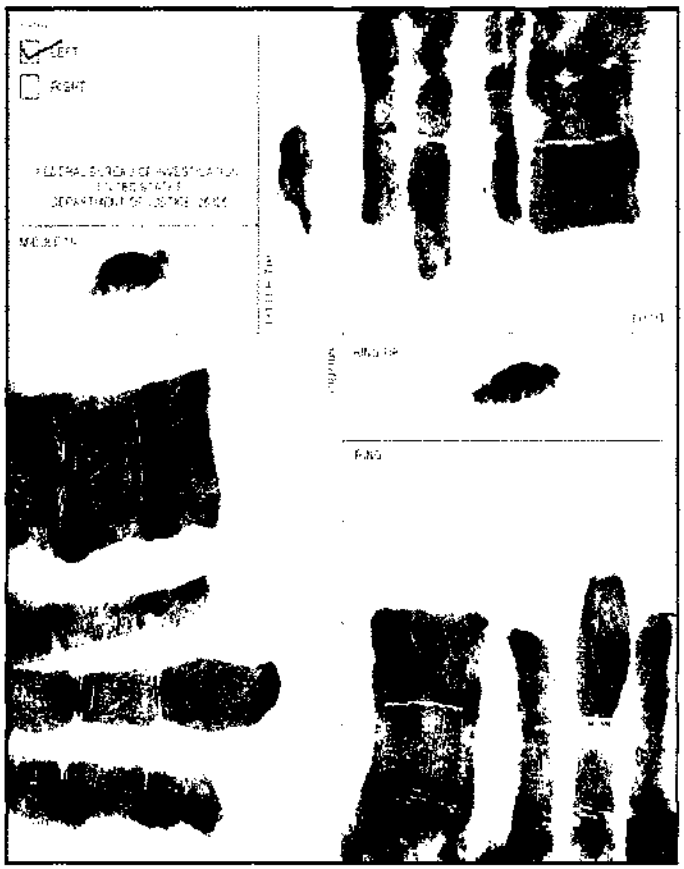
Form SS-la: Supplemental Finger and Palmprint Card (Back Side)
• This guide is for print orientation purposes only

Little tip:
Orient tip of little finger in direction of text within the capture block.

Note: Select Left or Right hand. All impressions must be captured in a vertical, upright position.

Middle Tip:
Orient tip of middle finger in direction of text within the capture block.

Middle:
Orient middle finger in direction of text within the capture block.
Capture one *fully rolled* middle finger impression.
Capture one *left edge* middle finger impression.
Capture one *flat* middle finger impression.
Capture one *right edge* middle finger impression.



Little:
Orient little finger in direction of text within the capture block.
Capture one *fully rolled* little finger impression.
Capture one *left edge* little finger impression.
Capture one *flat* little finger impression.
Capture one *right edge* little finger impression.

Ring Tip:
Orient tip of ring finger in direction of text within the capture block.

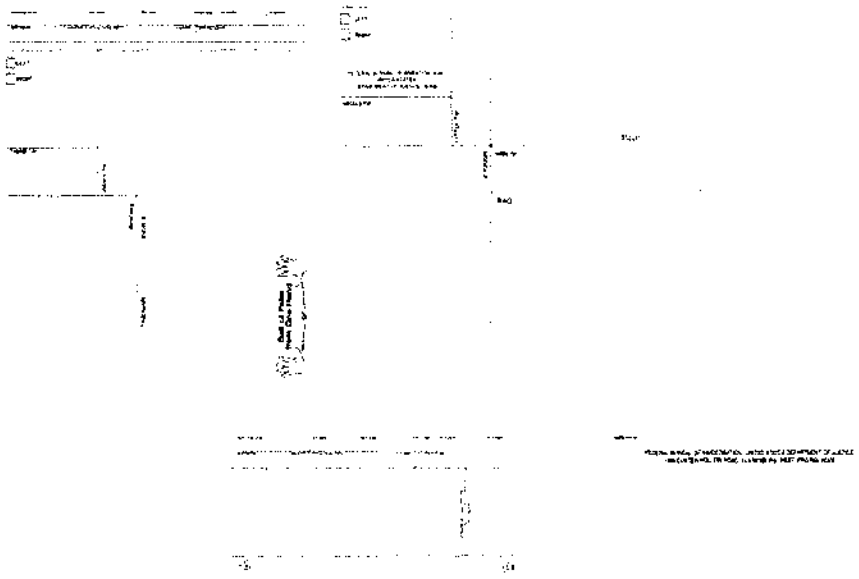
Ring:
Orient ring finger in direction of text within the capture block.
Capture one *fully rolled* ring finger impression.
Capture one *left edge* ring finger impression.
Capture one *flat* ring finger impression.
Capture one *right edge* ring finger impression.

Contact and Ordering Information

As of July 2010, the FD-884 (10-28-99) and FD-884a (5-07-07) have been revised and will be available in the near future. Existing cards will be accepted; however, please ensure that the capture of the friction ridge information is oriented as depicted within this guide

- To order revised FD-884 (7-02-10) (Palmprint) and revised FD-884a (7-02-10) (Supplemental Finger and Palmprint) cards at no charge from the FBI, contact the Fingerprint Supply Center at 304-625-3983 or visit our website: www.fbi.gov/hq/cjisd/forms/orderingfps.htm
- For livescan submissions, please refer to the Electronic Biometric Transmission Specification (EBTS), available at www.fbibiospecs.org
- Additional questions: Contact the Customer Service Group at 304-625-5590 or liaison@leo.gov
- Submit comments regarding palmprint cards and/or this guide to the Criminal Justice Information Services Division at latentservices@leo.gov

Contact and Ordering Information



Revised 9/2010