DRAFT Writing Guidelines to Develop an MOU for Interoperable Automated Fingerprint Identification Systems

Latent Print AFIS Interoperability
Working Group

LAW ENFORCEMENT STANDARDS OFFICE

OLES
LAW ENFORCEMENT
STANDARDS OFFICE

A division of

NIST

National Institute of Standards and Technology

Enter Once, Search Many

Table of Contents

FOREWORD

This is one of a series of documents prepared by the Latent Print Automated Fingerprint Identification Systems (AFIS) Interoperability Working Group. The purpose of these documents is to provide guidance and a framework to those involved in the identification process who may be tasked to be a project leader or member of a working group for an AFIS replacement, upgrade, or move to a more biometrics-based identification process.

Each agency has its own procedures as well as policies and laws that are applicable in the procurement process. The information contained in these documents should be considered as complementary.

The Latent Print AFIS Interoperability Working Group

The lack of latent print interoperability and the subsequent missed opportunities to make identifications have been long recognized as serious issues within the identification community. Latent print examiners, AFIS managers, vendors, governmental agencies, and professional organizations have explored opportunities to improve interoperability. Since the introduction of AFIS databases in the 1980s and the Federal Bureau of Investigation's (FBI's) Integrated Automated Fingerprint Identification System (IAFIS) in the late 1990s, latent print identifications have risen on a hierarchical level but not on a peer-to-peer basis.

As part of a National Institute of Justice (NIJ)/National Institute of Standards and Technology (NIST) effort to address the lack of AFIS latent interoperability, the Law Enforcement Standards Office (OLES) formed the Latent Print AFIS Interoperability Working Group. The mission of this Working Group is to improve latent print AFIS interoperability by developing a clear understanding of the issues and challenges to latent print AFIS interoperability and to identify collaborative ways to actively address this national problem.

The first meeting of the Working Group was held in April 2008. The release in February 2009 of the National Academies of Sciences' report, *Strengthening Forensic Science in the United States: A Path Forward*,[1] gave further support to the issue at a national level.

The Working Group consists of federal, state, and local representatives as well as vendors and other members of the identification community. These include the following:

[1] National Academy of Sciences, National Research Council, Committee on Identifying the Needs of the Forensic Science Community. *Strengthening Forensic Science in the United States: A Path Forward.* National Academies Press, 2009.

State and Local Representation
Broward County, Florida, Sheriff's Office
Culver City, California, Police Department
Illinois State Police, Forensic Science Center at Chicago
Los Angeles County, California, Sheriff's Department
New Hampshire Division of State Police Forensic Laboratory
New York State Division of Criminal Justice Services
Nlets
San Francisco, California, Police Department
Santa Monica, California, Police Department
South Carolina Crime Information Center
Texas Department of Public Safety
Western Identification Network, Inc.

Federal Representation
Department of Homeland Security
FBI Criminal Justice Information Services Division
NIJ Office of Science and Technology
NIST Information Technology Laboratory
NIST Law Enforcement Standards Office

AFIS Technical Advisors and Vendor Representatives

While many individuals contributed to the success of this project, the following are noted for having made significant contributions of their time, talent, and vision:

Susan Ballou	National Institute of Standards and Technology
Anthony Clay	United States Secret Service
Joi Dickerson	Culver City, California, Police Department
Mike Garris	National Institute of Standards and Technology
Peter T. Higgins	Higgins & Associates, International
Janet Hoin	New York State Division of Criminal Justice Services
Lisa Jackson	Santa Monica, California, Police Department
Mike Lesko	Texas Department of Public Safety
Joe Morrissey	New York State Division of Criminal Justice Services
Leo Norton	Los Angeles County, California, Sheriff's Department.
Beth Owens	Franklin County, Ohio, Sheriff's Office
Joe Polski	International Association for Identification (Ret.)

The objectives of the Working Group in the preparation of these documents were to:

- □ Define the issues and challenges to latent print AFIS interoperability
- □ Identify opportunities to actively address latent print interoperability

❑ Develop guidelines to provide guidance on technical and administrative issues

The Working Group developed this and other documents to meet the needs of latent print examiners, AFIS users, managers, vendors, and policy makers to establish interagency latent print AFIS interoperability. This document is one in a series of reference documents to help agencies achieve interoperability, located at http://www.fingerprint.nist.gov/.

HOW TO USE THIS GUIDE

This document is intended to be used as a guide to developing a latent AFIS Interoperability Memorandum of Understanding (MOU) between two or more agencies. For the purposes of this document, an MOU and Memorandum of Agreement should be considered interchangeable. The document is laid out in a common MOU format and includes suggested headings for each section. Within each section are established questions that can be considered during the development of the MOU. In the format and headings, this document incorporates the key elements of interoperability.

The example language, indicated with the image of a keyboard in the left margin, can be used for reference purposes and may or may not address applicable issues based on the varied needs of differing jurisdictions. This sample language is meant for guidance and illustration purposes toward a specific MOU item and should *not* be taken literally. Language within each individually created MOU will need to be modified and crafted to address the specific needs of the agencies involved in the agreement.

The partnerships that may be created by an MOU can be as varied as there are political entities. There is no "one size fits all" approach. In the following narrative, there is an emphasis on those collaborative efforts in which two or more agencies agree to pool their resources and create a new entity, such as a consortium, responsible for the administrative, legal, and financial obligations of the participating parties. There is adequate direction in the document to meet these issues.

The more common scenario may be the one in which two agencies are willing to share limited services and are looking for more simple guidance. Here, the reader may look directly at:

- ❑ Attachment I: Template for a Latent Print Processing Agreement Between the Hosting Agency and Requesting Agency
- ❑ Attachment II: Operational Responsibilities Template
- ❑ Attachment III: Automated Fingerprint/Biometric Identification System User Qualifications Guidelines Template

This document does not address every issue that may arise between different agencies who are seeking to create an MOU. It will need to be customized to the capabilities and resources for which it is established and should consider any unique concerns, characteristics, and needs of the participating agencies. This document is one in a series of reference documents to help agencies achieve interoperability, located at http://www.fingerprint.nist.gov/.

Potential guidance for governance may be available through existing agreements already endorsed by a specific agency, such as Nlets agreements, Criminal Justice Information

Services (CJIS) Wide Area Network (WAN) user agreements, or Joint Automated Booking System interface agreements.

GETTING STARTED

Both parties should understand why it would be advisable to create an MOU. Persons involved with the development of the MOU will need to understand the political implications and the impact of connectivity or sharing of resources. They should determine who has executive authority for the signing and execution of the MOU and who should effectively lead the group in this process.

In preparation for the creation of an MOU, it will be necessary to ascertain in detail with specific references the parties involved in the agreement, including addresses and points of contact (POCs). The participating parties who should be considered as integral in the development of the document could include:

- □ Operations personnel
- □ Managers
- □ Legal experts
- □ Technical staff members
- □ Vendors

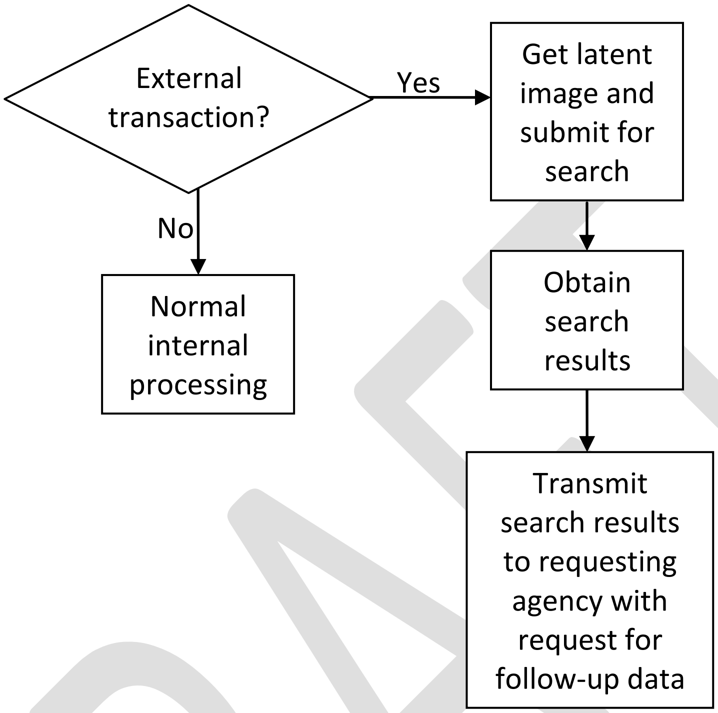
Workflow

It might prove helpful to develop a workflow to visualize the processes. This document should describe what business logic (workflow) would be required to be consistent with the latent interoperability search transactions either agreed upon or considered by the agency(ies) examining the implementation of latent interoperability.

Parties to the agreement should examine their systems and business logic and determine the workflow changes required to perform tasks such as:

- □ Accepting external latent transactions
- □ Adding external latents to internal Unsolved Latent File (ULF), or specifications for not adding external latents
- □ Reporting a match list back to the external submitting agency
- □ Establishing a threshold score for reporting a candidate back to the agency or returning a “no hit”
- □ Producing an error report for transaction responses
- □ Reporting successful matches back to the cooperating agency that ran the search
- □ Collecting and reporting metrics between the cooperating agencies
- □ Establishing business rules for external search compared to internal searches (Will all internal workflow be applicable to external searches? Does internal latent search require supervisor assignment?)

Process for Searching Latent Prints


External transaction?
Yes
Get latent image and submit for search
Obtain search results
Transmit search results to requesting agency with request for follow-up data
No
Normal internal processing

1. Introduction Section

The Introduction section of the MOU helps the reader to understand the agreement. This section should be a simple explanation of the agreement and why it is useful. It does not need to include details about past efforts or to discuss how the agencies reached this level of agreement. Depending on the agency's needs, a single agreement may be sufficient for a bi-directional data exchange. If there are different service agreements for each party, they should be defined.

- ❑ What agencies are participating in the MOU?
- ❑ For what capability or resource is this MOU being created?
- ❑ Why is this MOU necessary?
- ❑ What agreements are set forth by this MOU?
- ❑ Under what authority is this agreement being executed?

Example Language

This MOU was established for latent print AFIS interoperability between *[insert names of all parties: county/region/state]*. Criminal justice agencies recognize the need for latent print examiners or units to have the ability to search latent print data between two or more systems correctly and with minimal loss of accuracy, returning the results for review by the requesting agency. By definition of AFIS latent interoperability, the intent is for the sender to invoke all human effort while the receiver does not expend any human effort but requires significant machine effort. The agreement set forth in this MOU should detail all applicable aspects of latent print interoperability, including transmission methods, security, transaction formats, quantity and types of transactions, and support. Execution of this MOU will allow greater opportunity for identifications. This MOU is being implemented under the following authority: *[list applicable state or federal laws]*.

2. Purpose Section

The Purpose section of the MOU should be a concise statement discussing the intention of the new or proposed capability that makes the MOU necessary. It explains how the agencies involved will use the new capability and under what circumstances.

Example Language

The purpose of this MOU is to help all member agencies work cooperatively to establish a seamless, integrated system of *[statewide/countywide/region-wide]* information-sharing technology and services. The MOU will allow direct communications between the participating agencies when dealing with identification of latent prints. The sharing of data between the participating agencies will enhance the safety of the citizens of *[name geographic region]* due to the expanded search capabilities. This MOU intends to:

- ❑ Identify the roles and responsibilities of those participating agencies to guarantee continued success of the program within the *[name geographic region]*; and
- ❑ Ensure participating agencies are aware of the capabilities, limitations, and equipment maintenance responsibilities of the network.

3. Scope Section

The Scope section of the MOU is intended to provide the parameters of the latent AFIS interoperability solution and should include the following set of specifications and requirements:

- □ Defined periods of engagement (expiration, termination, and renewal)
- □ Agreement on transmission methods, connectivity, and security
- □ Agreement on transaction formats
- □ Agreement on data to be searched, returned, and retained
- □ Agreement on corrective actions
- □ Deliverables (reporting, metrics, statistics, success stories)
- □ Troubleshooting, help desk, outreach, support
- □ Security/privacy disclosures
- □ Suspension of access
- □ Agreement on number of ULF searches per day
- □ Agreement on error messaging notification
- □ Agreement on the forwarding of cascaded search results if the receiving agency has existing MOU agreements with other agencies

Agencies should agree upon operating procedures and include them as an appendix to the MOU.

Example Language

Defined periods of engagement (expiration, termination, and renewal)

This agreement will become effective on *[insert date]* and shall continue for *[insert # of years/months]*. This agreement shall automatically renew on an annual basis for *[define term of agreement]* unless the parties notify each other in writing, with 30 days notice, of their intent to terminate the agreement. After the *[define term of agreement]*, review and approval is required.

Example Language

Agreement on transmission methods, connectivity, and security
Agencies will use the following connectivity methods: *[selected from CJIS WAN, Nlets, Law Enforcement Online, a virtual private network (VPN), or other]*.

Example Language

Agreement on transaction formats
Agencies will use the following standard transaction formats: *[selected from CJIS's Electronic Biometric Transmission Specification (EBTS), American National Standards Institute (ANSI)/NIST, or the Latent Interoperability Transmission Standard (LITS) and specifying specific versions]*.

Example Language

Agreement on data to be searched, returned, and retained
Agencies will search latent prints as defined in the chart below:

Function	**Max Number of Inquiries/Day**	**Priority Status**	**Response Time**
Single latent fingerprint search vs. ten-print fingerprint repository (criminal only, civil only, both criminal and civil, special repositories) (ten-print searchable repository being rolled fingerprints, plain impressions, or both) (single record, multi-record per individual) (image- vs. minutiae-based search) (filtering, no filtering criteria permitted)			
Multi-latent fingerprint search vs. ten-print fingerprint repository (criminal only, civil only, both criminal and civil, special repositories) (ten-print searchable repository being rolled fingerprints, plain impressions, or both) (single record, multi-record per individual) (image- vs. minutiae-based search) (filtering, no filtering criteria permitted)			
Single latent palm print search vs. palm print repository (criminal only, civil only, both criminal and civil, special repositories) (assumes two palms for each individual) (single record, multi-record per individual) (image- vs. minutiae-based search) (filtering, no filtering criteria permitted)			

Descriptive-based search (physical description, e.g., gender, race, age, height, etc., of individual along with other defined delimiters, but no latent print image or minutiae) (other defined delimiters, such as classification, finger position, geographic region, crime type, etc.)			
Add to ULF (latent fingerprint, latent palm print) (image, minutiae, both) (descriptive delimiters)			
Ten-print search vs. ULF			
Palm print search vs. ULF			
Latent fingerprint search vs. ULF			
Latent palm print vs. ULF			

Agencies agree to the search data types, data retention, and result retention for *[define a period of time]*. For the purposes of latent print case documentation and legal considerations, the result retention requirement is a recording of the search data and results record. The length of time, the content, and how to obtain the record should be clearly described.

Example Language

Agreement on corrective actions
The parties agree to provide each other the opportunity to take corrective actions or to exercise the ability to resolve any incidents that may arise during the term of this agreement.

Example Language

Deliverables (reporting, metrics, statistics, success stories)
Each member agency shall provide formal and ad hoc report relating to the interoperability capability as a result of this agreement. The reports may include: *[define the types of data]*

Example Language

Troubleshooting, help desk, outreach, support
Each agency is responsible for maintaining its system availability and for providing a POC for technical support. Designated POC: *[insert name].*

Each agency needs to provide notification of planned outages within *[define length of prior notification]* and extended unplanned system outages within [*define length of time, e.g., # of hours*].

Example Language

Security/privacy disclosures

[Cite relevant privacy rules/regulations]. Neither agency will disclose the results of searches without coordinating with the other party to this agreement. *[Specify individual means of coordinating results, e.g., telephonic or written communication].*

Example Language

Suspension of access

The parties may suspend access to each other "for cause" or breach of the agreement for the following reasons:

1. Disclosure of protected information (personally identifiable information)
2. Breach of security of the system
3. Any misuse
4. Failure to abide by financial arrangements
5. *[Insert additional reasons for suspension of access]*

Example Language

Agreement on number of ULF searches per day

The parties of the agreement will agree on a maximum of *[insert number]* ULF searches per day.

Example Language

Agreement on error messaging notification

Agencies shall provide notification and definition of transaction-related errors within *[define time period]*.

Example Language

Agreement on the forwarding of cascaded search results if receiving agency has existing MOU agreements with other agencies

Agencies agree to use existing MOUs to conduct cascaded searches. The receiving agency should return all cascaded search results back to the original agency that initiated the search.

4. Policy Section

The Policy section of the MOU should contain policy definitions that are agreed to by the member agencies. Policies to be considered should include the following:

- ❑ **Data security.** Agencies must provide secure and controlled access to data exchanged as a part of the latent interoperability solution. This data exchange is secured using technologies such as a secured connection and authorized access. Each agency should agree to adhere to the more stringent security policy of the member agencies.
- ❑ **Privacy Act considerations and release of data parameters (third-party sharing).** The laws, rules, and regulations governing the dissemination of information must be understood and described.
- ❑ **Record retention/deletion requirements.** The search data retention period and the contents of the search/results record need to be stated. For purposes of latent print case documentation and legal considerations, a recording of the search data and results record need to be defined. The length of time, the content, and how to obtain the record should be clearly described. Agreement on how sealed records should be handled should be developed.
- ❑ **Availability.** The availability of the AFIS should be described. If the receiving AFIS restricts access during certain periods (e.g., peak load times during each day, weekends, or predetermined maintenance periods), then these periods should be indicated.
- ❑ **Liability.** Legal liabilities associated with accessing an AFIS must be documented and understood. There is a wide range of matters to be covered under this topic, and the agency's legal department should be directly involved. Topics at the system level, such as authorization, data security, and misuse, need to be addressed. Other topics related to system performance and accuracy should be addressed. Specifically, it should address the liability associated with searches having negative results when, in fact, positive results should have been achieved, i.e., a failure of the AFIS to provide the correct candidate in a response to an inquiry when the correct candidate is in the database.
- ❑ **Criminal/civil database searching limitations and responses.** Participating agencies should agree as to the policies for accessing criminal, civil, and/or special databases (e.g., bank robbery or terrorist files) and enrolling records into the ULF. If an individual is being selected as a candidate as a result of an external inquiry and that individual's record is protected from dissemination (in whole or in part), the process in which this matter is handled must be described.
- ❑ **Qualifications of users (full spectrum).** Participating agencies should agree to minimum qualifications for users allowed access to the interoperability capability. This may include training, certification, and competency testing. (See Attachment III: Automated Fingerprint/Biometric Identification System User Qualifications Guidelines Template.)

5. Oversight Section

The Oversight section describes the governance structure under which the MOU will be administered. It may also describe how execution and implementation of this solution could be integrated into an existing governmental structure.

Questions to consider:

- □ What governance structure oversees the use of this capability/resource and enforces all requirements of this MOU?
- □ Who is the chair of this governance structure and how is he/she appointed?
- □ What are the participation requirements in this governance structure of agencies entering this MOU?
- □ How are issues affecting policy, recommendations, and/or subsequent changes resolved by the governance structure?
- □ What is the decision-making process within the governance structure?
- □ How do individual agencies establish oversight authority for the capability/resource?
- □ How should the oversight authority establish consensus?

Example Language

Oversight of the AFIS latent interoperability agreement is administered through the Interoperability Committee. The Committee may be co-chaired by an appointee of each agency. Each participating agency participating may provide a representative to the Interoperability Committee after entering into this MOU. Any issues affecting policy, recommendations, and/or subsequent changes that alter the purpose of the AFIS latent interoperability agreement may be implemented only after a consensus is reached by the Interoperability Committee. Accordingly, each agency may establish oversight authority and may identify the level of delegation in reference to use of the AFIS latent print interoperability solution.

6. Compliance Section

The Compliance section of the MOU assigns responsibility to agencies to develop operational responsibilities and to ensure they are followed. A functional and performance test to validate that interoperability has been implemented in accordance with this MOU will be conducted on each member’s system.

Questions to consider:

- □ Who is responsible for ensuring that the operational responsibilities associated with this capability/resource are followed and that individual agency personnel are trained appropriately?
- □ How will compliance be ensured?

Example Language

It is the responsibility of agency heads to ensure that the AFIS latent interoperability agreement's operational responsibilities are followed when necessary and to ensure that agency personnel are trained appropriately. Compliance is ensured through *[define time period]* audits conducted by each agency.

7. Updates to the MOU Section

The Updates to the MOU section describes how updates can be made to the MOU. It includes information such as who has the authority to update the MOU, how updates will be made, how participating agencies will be notified of updates, and the types of updates that will require signatures of all participating agencies.

Questions to consider:

- □ Who has the authority to update/modify this MOU?
- □ How will this MOU be updated/modified?
- □ Will updates/modifications require this MOU to have a new signature page that verifies the understanding of changes by each participating agency?
- □ Who maintains original documentation?

Example Language

Updates will take place after the *[insert authority body here]* meets and gains consensus on proposed changes. It is then the responsibility of the Interoperability Committee to decide the best possible method of dissemination to all affected agencies. In the event that a proposed change or technical upgrade to the latent AFIS degrades the capability or changes the purpose of the agreement, a new signature page verifying the understanding of changes will be required.

8. Financial Considerations Section

The Financial Considerations section of the MOU should describe how the interoperability services will be funded. There are two potential payment arrangements that agencies can consider:

- ❑ **Shared services.** No costs are exchanged. Each agency is wholly responsible for the cost of the searches conducted on their systems.
- ❑ **User fee services.** Cost per search is agreed to by the member agencies on the basis of the increased cost resulting from the interoperability workload. If a fee for service is to be charged, the terms and conditions must be clearly stated. There are numerous approaches in which fees for service can be invoked. For example, each functional capability could have a distinct fee for service for each transaction. Or, a single monthly fee may be stated regardless of the number of inquiries submitted.

Example Language

Shared Services

Financial responsibility. Each member agency or authorized user is responsible for the cost of acquiring and maintaining the necessary hardware and licensed software to participate in the project. Nothing in this MOU requires any agency to fund the activities of any other member agency or authorized user.

Grants. Any member agency or authorized user may individually or collectively apply for grant funding for this system. Monies applied for by an individual agency or a partnership of agencies shall in no way be controlled by or fall under the jurisdiction of this MOU, nor shall such funds be considered pass-through funds for the fiscal agent. Only where the *[insert authority body here]* as a group applies for a grant or other federal funds will the fiscal agent be considered a pass-through entity. The fiscal agent will not be responsible for initial costs in applying for any grants or funding on behalf of *[insert authority body here]*.

Fiscal agent. The Interoperability Committee may appoint a fiscal agent(s). The fiscal agent(s) shall report on fiscal matters involving the *[insert authority body here]*. A review of the *[insert authority body here]* accounts, maintained by the fiscal agent, will be completed at the discretion of the Committee and paid for with Committee funds.

Shared costs. Under a shared services agreement, member agencies will agree to a number of searches and database additions in a manner that is satisfactory to each agency and is defined as part of this MOU. Once this agreement is in place, each party should be wholly responsible for any additional costs of this agreement.

Example Language

User Fee Services

The total cost of providing the additional interoperability services is divided by the expected workload to calculate user fees as incurred per search and/or addition.

Payment to constitute current expenditures. Member agencies acknowledge and agree that all payment obligations under this MOU are current expenditures of member agencies, payable in the fiscal year for which funds are appropriated for payment thereof. Member agencies' obligations under this MOU shall be from year to year only and shall not constitute a multiple-fiscal year direct or indirect debt or other financial obligation of member agencies within the meaning of *[reference any state constitution if applicable]*.

Attachment I:

Template for a Latent Print Processing Agreement between the Hosting Agency and the Requesting Agency

This template contains specific language that may be inserted into an MOU between two agencies. The agencies should carefully review this language to ensure it correctly fits the desired outcome and should freely add to this language where necessary.

Example Language

This Agreement, dated *[insert date]*, is made between *[insert name and address of agency A]* (hereinafter referred to as the Hosting Agency) and *[insert name and address of agency B]*, (hereinafter referred to as the Requesting Agency). The foregoing are collectively referred to as the "Parties."

WHEREAS, the Hosting Agency has purchased equipment and software licenses to enhance the latent print processing capabilities at the Hosting Agency, and the Hosting Agency has an interest in providing for the security of the equipment and data and in abiding by the contractual warranty conditions and software licenses imposed by the automated fingerprint identification system (AFIS) Vendor, *[insert vendor name]*, (hereinafter referred to as the Vendor), and;

WHEREAS, the Requesting Agency has requested to use the equipment and software license purchased by the Hosting Agency to improve its latent print processing through interoperability.

In consideration of the mutual obligations contained herein, NOW, THEREFORE, it is agreed by and between the Hosting Agency and the Requesting Agency as follows:

1. Legal Requirements

The Parties agree that this Agreement shall be subject to the *[insert state, county, city, etc.]* standard contract clauses. *(Optional: These may be set forth in an Appendix and attached as part of this Agreement.)*

The Parties agree to abide by the guidelines and responsibilities specified in the Requesting Agency's Responsibilities Document, attached hereto as Appendix *[insert appendix letter]* and made a part of this Agreement as if fully set forth.

2. Equipment

Title to the Hosting Agency's AFIS software, for which the Hosting Agency has obtained the necessary licenses, shall remain the exclusive property of *[insert vendor name]*.

Approved expansion equipment installed after the original equipment installation and all other equipment shall remain the property of the party that purchases such equipment.

3. Identification and Classification Procedures

When identification results using the Hosting Agency's AFIS, the Requesting Agency may separately request criminal history record information from the Hosting Agency criminal history files via the Hosting Agency's recognized communication links.

All such criminal history information shall remain subject to the terms of any existing Use and Dissemination Agreement between the Hosting Agency and the Requesting Agency governing the exchange of criminal history record information.

Secondary dissemination of criminal history record information is not permitted for any reason except for the transmittal to another law enforcement agency for criminal investigation purposes.

4. Conditions of Use Provisions

The Hosting Agency may, at its option, suspend the provision of interoperable latent print AFIS services to the Requesting Agency if the Requesting Agency knowingly permits one or more of the following situations to exist, which may either compromise the security of Vendor information or which may necessitate replacement or repair to correct system failure or possible system failure:

a) Failure to continually provide or maintain a suitable installation environment as indicated in the guidelines contained within Appendix *[insert appendix letter]*.

b) Use of supplies or materials *not approved* by the Hosting Agency or inappropriate use of the Hosting Agency-approved materials.

c) Neglect or misuse of the equipment or system, or the use or attempted use of the equipment or system for purposes other than as the Requesting Agency.

d) Alterations, attachments, conversions, upgrades, downgrades, or enhancements to the system or any other action that causes any deviation from the Hosting Agency's system as designed by the Vendor.

e) Attachments, including interconnection of the system by mechanical or electrical means to any other machine, equipment, or device unless the Requesting Agency has obtained formal written approval from the Hosting Agency.

f) Maintenance or repair of the system performed by any party not authorized by the Hosting Agency.

g) Intentional or negligent damage to the system by personnel of the Requesting Agency or any other third party.

h) Allowing any unauthorized Requesting Agency personnel or any unauthorized third party, for reasons other than preapproved maintenance procedures, to attempt to gain or to actually gain access to the components of the system software that has been encased in locked subsystems of the system.

i) Disclosure of, duplication of, or the unauthorized use of any information that the Vendor has designated as proprietary information for the system. Such proprietary information shall include the system software, including any enhancements, any items that may have passed to the Hosting Agency pursuant to the Agreement with the Vendor, and any other information that the Vendor has specifically designated as proprietary.

j) Failure to maintain responsibility for any replacement or repair costs that are directly attributable to the situations that have been listed above in subparagraph *a* through *i* and that may be imposed upon the Hosting Agency by the Vendor, or failure to maintain responsibility for any damages resulting from the disclosure, duplication, or unauthorized use of proprietary information described above in subparagraph *i.*

5. Term and Termination

This Agreement will have a term of *[insert #]* years from execution by the Parties, unless terminated as provided herein. The Parties reserve the right to amend the Agreement from time to time as needed, including removal of all or part of the equipment in response to non-usage or extremely low usage levels. All amendments or renewals shall be written and signed by the Parties.

The Hosting Agency may, at its discretion, cancel this Agreement at any time, upon thirty (30) days written notice, if the Requesting Agency fails to comply with the terms contained herein or if funds for the continued operation of the Hosting Agency's System are not appropriated or in the event of the cancellation of the agreement between the Hosting Agency and the Vendor.

6. Use of the Hosting Agency's Equipment

The Requesting Agency personnel or the other system users authorized by the Requesting Agency shall not use any of the Hosting Agency's AFIS equipment until and unless authorized by the Hosting Agency. The Requesting Agency agrees to take reasonable precautions to prevent unauthorized persons from accessing the Hosting Agency's AFIS equipment or software.

7. Notification of Action

The Requesting Agency shall notify the Hosting Agency in writing within fifteen (15) days after an initial *notification* of any legal actions brought by a third party against the Hosting Agency, the Vendor, or the Requesting Agency, in an action involving the Hosting Agency's AFIS.

8. Indemnification of the Hosting Agency

The Requesting Agency, to the extent permitted by state or Federal law, agrees to indemnify and save harmless the Hosting Agency, its officers, and its employees, from and against any and all claims, demands, actions, suits, and proceedings brought by others arising out of the terms of this Agreement resulting from the negligence or other tortious conduct of the Requesting Agency, including but not limited to any liability for loss or damage by reason of any claim of false imprisonment or arrest.

9. Effective Date

This Agreement shall become effective when signed by the executive official of the Hosting Agency or designee and the executive official of the agency designated as the Requesting Agency having the authority to contract on behalf of the Requesting Agency.

THE HOSTING AGENCY	THE REQUESTING AGENCY
By: ______________________________	By: ______________________________
Title: ____________________________	Title: ____________________________
Date: ____________________________	Date: ____________________________

ACKNOWLEDGMENT CLAUSE

State of ______________________________

County of _____________________________

On the *[insert date]* day of *[insert month]* in the year *[insert year]* before me personally came *[insert name]* to me known, who, being by me duly sworn, deposes and says that s/he is the *[insert title]* of the *[insert agency]*, the entity that executed the above instrument, that s/he was authorized by and did execute the same at the direction of said entity, and that s/he signed his/her name thereto.

____
Notary Public

Attachment II:

Operational Responsibilities Template

The example template below provides possible text to be used in developing the Operational Responsibilities document. Agencies may copy this text directly but should review it carefully to agree on the structure of the agreement. Because this section would likely be included as an attachment to an MOU, no separate signature page has been included.

Example Language

1. Introduction

The purpose of this document is to summarize the responsibilities of the parties involved in the operation of the Latent Print Processing Agreement.

The relevant parties are *[insert name of agency A]* (hereinafter referred to as the Hosting Agency) and *[insert name of agency B]* (hereinafter referred to as the Requesting Agency). The foregoing are collectively referred to as Parties.

The document describes the relationship of the Hosting Agency and the Requesting Agency for a number of functions.

2. Organizational Responsibilities

Responsibilities of the Hosting Agency

The Hosting Agency shall:

- ❑ Accept and retain title to the AFIS equipment and software licenses purchased by the Hosting Agency for use at the site
- ❑ Implement system-wide changes
- ❑ Provide staff support to the Requesting Agency as necessary
- ❑ Serve as prime contact with the Vendor for AFIS hardware and software
- ❑ Make no publicity releases resulting from the use of AFIS by the Requesting Agency without prior approval of the Requesting Agency to determine that no un-apprehended suspects would be directly or indirectly identified
- ❑ Confer as needed

Responsibilities of the Requesting Agency

The Requesting Agency shall:

- ❑ Identify potential uses within boundaries
- ❑ Appoint a manager who will act as a liaison between the Hosting Agency and the Requesting Agency. Notification of manager appointments should be via hard-copy message to the manager at the Hosting Agency. The manager shall participate in meetings as required.
- ❑ Recommend procedural changes to the Hosting Agency
- ❑ Comply with the Hosting Agency's requirements for safeguards against improper use of proprietary information, including ensuring information is properly secured during transmission within the local network
- ❑ If it is not the investigating agency, make no publicity releases resulting from the use of AFIS at the Requesting Agency without prior approval of the investigating agency to ensure that no un-apprehended suspects would be directly or indirectly identified
- ❑ Submit appropriate reports and other necessary data as required by the Hosting Agency

3. System Operation and Access

The System Operation and Access section contains items such as maintenance procedures, warranty provisions, security of equipment, physical access to equipment, and processing priorities.

Responsibilities of the Hosting Agency

The Hosting Agency shall:

- ❑ Administer a system-wide maintenance contract with the Vendor
- ❑ Establish system-wide processing priorities and revise as necessary
- ❑ Monitor AFIS usage and system processes at the Requesting Agency
- ❑ Provide a help desk accessible to report problems and outages
- ❑ Provide search capabilities to the Requesting Agency in a manner so as not to interfere with the Hosting Agency's normal workflow. The Requesting Agency's searches will take a lower priority and may be restricted to off-peak and weekends. *(Option: Search shall be limited to between [insert time] to [insert time] during weekdays and [insert time] to [insert time] during weekends.)*

- ❑ The Hosting Agency may restrict the number of latent to ten-print searches to *[insert #]* per day or *[insert #]* per week.
- ❑ The Hosting Agency may restrict the number of ten-print to latent searches to *[insert #]* per day or *[insert #]* per week.
- ❑ The Hosting Agency may restrict the number of latent palm to palm searches to *[insert #]* per day or *[insert #]* per week.
- ❑ The Hosting Agency may restrict the number of latent palm to latent palm searches to *[insert #]* per day or *[insert #]* per week.

Responsibilities of the Requesting Agency

The Requesting Agency shall:

- ❑ Be open during normal business hours
- ❑ Promote maximum effective usage
- ❑ Follow all approved AFIS procedures regarding processing of Unsolved Latent (UL) Cases (if permitted)
- ❑ Conduct periodic validation of case status of the Unsolved Latent File (ULF) (UL and UL palms if permitted) as requested by the Hosting Agency
- ❑ Schedule preventive maintenance with the Vendor and inform the Hosting Agency and users of scheduled downtime, complying with trouble reporting procedures
- ❑ Provide for restricted access to the AFIS equipment area and for the physical security of AFIS equipment, including transmission facilities and equipment
- ❑ Comply with all the AFIS "conditions of use" provisions contained in the body of this Agreement
- ❑ Provide verification of search candidates in a timely manner, not to exceed *[insert #]* days
- ❑ Process search result verifications in a timely manner, not to exceed *[insert #]* days
- ❑ Keep an updated list of authorized users
- ❑ Provide for a transfer of cases on the system when a qualified user retires, transfers, or leaves the agency, if appropriate
- ❑ Provide at least thirty (30) days advance notification of site relocation to the Hosting Agency

- □ Run such accuracy tests as may be required by the Hosting Agency and inform the Hosting Agency of any significant deviation in test results
- □ Follow such other procedures as the Hosting Agency may specify for the purpose of ensuring the security of the Hosting Agency information
- □ Remove cases from Hosting Agency within *[insert #]* days, if appropriate, or as requested

4. Site Preparation (If Applicable)

The Site Preparation section includes the major site preparation, evidence processing, and data communications responsibilities of the Parties, and is applicable only to a new Requesting Agency coming into the Agreement.

Responsibilities of the Hosting Agency

The Hosting Agency shall:

- □ Monitor the efforts of all entities involved in system installation. The Hosting Agency shall be the primary contact between the Requesting Agency and the Vendor for AFIS hardware and software, as well as telecommunications personnel.
- □ Determine the scheduling of the equipment installation, data communications network components, etc.

Responsibilities of the Requesting Agency

The Requesting Agency shall:

- □ Install and bear all costs for necessary AFIS telecommunications support associated with the AFIS equipment purchased by the Hosting Agency for use at the site, except where mutually agreed that the local entity elects to use existing facilities. Such equipment may include, but not be limited to, transmission lines, communications processors, network communications software, and communications monitors.
- □ Assume all cost involved in physically preparing the Requesting Agency to receive the equipment and associated power, heat, or conditioning and other operating costs with the exception of communications line.
- □ Designate a site liaison, specify the exact physical location for the terminal, and ensure that the site is ready for equipment/software installation.

5. Training

The Training section contains the major AFIS training responsibilities.

Responsibilities of the Hosting Agency

The Hosting Agency shall:

- □ Provide an orientation and training program on AFIS use to the Requesting Agency as needed.
- □ Provide additional information and/or training on any AFIS updates/changes.

Responsibilities of the Requesting Agency

The Requesting Agency shall:

- □ In conjunction with the manager at the Hosting Agency, coordinate AFIS-related training.
- □ Suggest new AFIS training procedures as needed.
- □ Subsequent to the Hosting Agency/Vendor–provided training session, provide training sessions to other Requesting Agency personnel and User Agency examiners. This should include instruction on the Requesting Agency's AFIS procedures. Conduct updates and refresher training as needed.
- □ Submit qualifications of users to the Hosting Agency for authorized AFIS user status (see User Qualifications).

6. UL Cases (If Permitted)

The UL Cases section details the responsibilities associated with the entering and verifying of cases in the ULF.

Responsibilities of the Requesting Agency

The Requesting Agency shall:

- □ Develop site criteria for the entry/deletion from the ULF.
- □ Enter cases into the UL and UL palm file that meet site criteria.
- □ Delete UL and UL palm cases after an identification has been made.
- □ Verify all UL fingerprint/ten-print and Unsolved Palm print (UP)/palm print cases within *[insert #]* days or *[insert #]* weeks of appearance in the verification queue.
- □ Verify all ten-print/ten-print and UP/UP cases within *[insert #]* days or

[insert #] weeks of appearance in the verification queue.

7. Cost (If Applicable)

The Cost section contains the parties' responsibilities for the cost of system components and services.

Responsibilities of the Hosting Agency

The Hosting Agency shall:

□ Retain title to all hardware purchased by the Hosting Agency.

□ Provide AFIS software licenses for AFIS equipment purchased by the Hosting Agency.

□ Provide a maintenance contract for AFIS equipment purchased by the Hosting Agency.

□ Provide all data communications network costs for AFIS equipment purchased by the Hosting Agency.

Responsibilities of the Requesting Agency

The Requesting Agency shall provide the following:

□ Salary and fringe benefits for personnel employed at the Requesting Agency.

□ All site modifications necessary to install AFIS.

□ Facility operating expenses (i.e., heat, light, and air conditioning).

□ Any local facility costs incurred.

□ Any charge for labor or travel imposed by the Vendor for violation of the AFIS "condition of use" provisions contained in the original agreement document or for damages caused by food or liquid spills.

□ Travel and per diem expenses connected with any meeting with the Hosting Agency.

Attachment III:

Automated Fingerprint/Biometric Identification System User Qualifications Guidelines Template

The template below provides language that could be used by agencies developing standards for AFIS user qualifications. Agencies should carefully review the text and amend where necessary to align with existing agreements and system requirements. Because this section would likely be an attachment to an MOU, no separate signature page is included.

Example Language

1. Purpose of the Guidelines

The purpose of these guidelines is to ensure a level of proficiency and expertise in latent print examiners who are authorized to conduct latent print searches on the automated fingerprint identification systems (AFIS) of other local and state criminal justice agencies. As latent print examiners, they must exhibit a high level of professionalism in latent print searches on their native systems. As a guest authorized to search another system, their conduct must be beyond question.

The relationship between the Hosting Agency and the Requesting Agency is built upon professional competency, adherence to procedures and regulations, and trust. Any perceived or actual action that violates these conditions could nullify the Agreement and terminate access.

2. Introduction

Access to latent print identification services at other locations provides additional opportunities to make latent print identifications on those individuals not identified on the native system. In addition to current cases, examiners may wish to search cold cases and those cases residing in the Unsolved Latent File (ULF).

This access allows a latent print examiner from the Requesting Agency to search the files of the Hosting Agency as a guest.

3. Training and Certification

To gain and maintain access to the latent print services of the Hosting Agency, latent print examiners of the Requesting Agency must exhibit competency in latent print identification, AFIS latent print processing of the native systems, and the unique features of programs and procedures used to search other Hosting systems. Examiners will need to be familiar with Extended Feature Set (EFS) user guidelines and Universal Latent Workstation procedures. Additionally, the examiners must be aware of and follow all procedures formally agreed to by the Hosting and Requesting Agencies.

Technical Training Required

- ❑ Minimum eighty (80) hours of training in latent print matters

Basic Experience Required

- ❑ Minimum two (2) years of full-time experience in the comparison and identification of latent print material and related matters; and
- ❑ Minimum one (1) year of experience in AFIS latent print searches

Education Requirements

- ❑ A Bachelor's Degree plus two (2) years of full-time experience; or
- ❑ An Associate's Degree or documentation of sixty (60) semester hours or ninety (90) quarter hours of college credits, plus three (3) years of full-time experience as a latent print examiner; or
- ❑ Four (4) years of full-time experience as a latent print examiner

Recognition as a Certified Latent Print Examiner by the International Association for Identification will serve to meet the technical training requirement and the two (2) year full-time experience requirement.

Competency in AFIS functionality includes all of the established workflow processing paths routinely used in the Requesting Agency, the Vendor's AFIS Latent Print Examiner Manual, and the primary function-oriented tasks that identify all of the specific system functions listed in the manual.

4. Nomination and Acceptance Process

The manager of the Requesting Agency will recommend to the manager of the Hosting Agency those examiners seeking authorization to latent print processing. The request should include information, including but not limited to, the following:

- ❑ Name
- ❑ Title/Rank
- ❑ Length of time as latent print examiner
- ❑ Credentials as noted above
- ❑ Level of access requested (e.g., limited or full)

The manager of the Hosting Agency will review the requests and respond within *[specify #]* days as to whether access has been granted, an effective termination date, and any sunset or other provisions.

5. Suspension/Termination of Access

Access to the Hosting Agency may be suspended or terminated under the general provisions of the Memorandum of Understanding.

Attachment IV:
Glossary of AFIS Terms

FOREWORD

This Glossary was developed from many sources. To support the standardization of use, wherever possible the acronyms, abbreviations, and their definitions were extracted from federal- and industry-recognized sources. There is no single nationally or internationally recognized glossary of AFIS terms. Like the differences between dictionaries, each source presents a slightly different wording for the same concept.

For example, there are differences in the definition of the word “glossary” between the *Merriam-Webster Online* (“a collection of textual glosses or of specialized terms with their meanings”), *Webster’s New World College Dictionary* (“a list of difficult, technical, or foreign terms with definitions or translations, as for some particular author, field of knowledge, etc., often included in alphabetical listing at the end of a textbook”), and the *Oxford Dictionaries Pro Online* (“an alphabetical list of terms or words found in or relating to a specific subject, text, or dialect, with explanations; a brief dictionary”). Is one right and the others wrong?

The reader is encouraged to refer to additional sources such as the Scientific Working Group on Friction Ridge Analysis, Study and Technology and other nationally recognized authoritative sources for complementary descriptions. Definitions that were pulled in whole or in part from other sources include a reference to that source in parentheses. A list of acronyms follows the definitions of terms.

ACCEPTANCE TESTING—1: A thorough test of an AFIS prior to taking ownership and making payment. 2: Those tests that are intended to determine that all equipment and software functions and complies with the contract specifications and to determine the reliability of the system. (ANSI/IAI)

ACCESS RIGHTS—Profile of a user composed of options to enable specific AFIS functions. For example, ten-print staff members cannot access latent print functions unless granted access rights to those functions.

ACCURACY—1: A software quality metric that provides those characteristics for required precision in calculations and outputs. 2: A measure of the AFIS's ability to place the correct mate within a specific position on the candidate list as a result of the matching process. (ANSI/IAI) 3: The closeness of agreement between the AFIS-generated representation of a fingerprint compared with the fingerprint it represents. (ANSI/IAI)

ACE-V—The process for identifying latent fingerprints, which involves Analysis, Comparison, Evaluation, and Verification:

- ❑ *Analysis* is the qualitative and quantitative assessment of Level 1, Level 2, and Level 3 Details to determine proportion, interrelationship, and value for individualization.
- ❑ During *Comparison*, the latent print examiner looks at the attributes noted during analysis for differences and agreement between the latent print and the known exemplar.
- ❑ *Evaluation* follows extensive comparison by making a determination if two impressions were made by the same source, not from the same source, or if the information is inconclusive. (A determination is made as to the results of the Comparison process. The fingerprint community accepts three conclusions: (a) the latent print and known exemplar were made by the same source, (b) the latent print and known exemplar were not made by the same source, or (c) a conclusive comparison could not be determined. This could be due to a lack of comparable area in the known exemplar or lack of clarity due to improperly recorded known exemplars.)
- ❑ *Verification* occurs when a second qualified examiner does an independent assessment of the latent print and known exemplar, utilizing the ACE process.

ACTIVITY LOG—A continuously updated record of system activity. (ANSI/IAI)

ALGORITHM—1: Mathematical routine used in computer processing. In AFIS processing, the matcher algorithm searches for relationships between the search print and ten-print. 2: Mathematical routine used in computer processing, e.g., an AFIS matching algorithm establishes the correlation of Level 2 Detail between fingerprints. (SWGFAST). 3: A step-by-step computational procedure for solving a problem. The system computer and other system components use algorithms to make decisions required to process and handle information. (ANSI/IAI)

ALPHANUMERIC—Non-image information related to a person, ten-print card, or latent case; may also be referred to as demographic data.

AMERICAN NATIONAL STANDARDS INSTITUTE—Institute founded in 1918 that administers U.S. voluntary standardization and conformity assessment.

ANALYSIS—1: The qualitative and quantitative assessment of Level 1, Level 2, and Level 3 Details to determine proportion, interrelationship, and value for individualization. 2: The first step in the ACE-V process.

ANSI/NIST STANDARD—Standard proposed by NIST and adopted by ANSI. For example, the ANSI/NIST-ITL standard *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information* is used by law enforcement, intelligence, military, and homeland security organizations throughout the world. The first version of this standard dates to 1986. Over the years, it has been updated and expanded to cover more biometric modalities beyond the original record type of fingerprint minutiae. (NIST)

ARTIFACT—1: Any distortion or alteration not in the original friction ridge impression produced by an external agent or action. 2: Any information not present in the original object or image inadvertently introduced by image capture, processing, compressions, transmission, display, or printing. (SWGFAST 2011)

AUTHENTICATION—1: A process to determine whether a digital image has been altered in any way since its capture. 2: A process used to determine whether an electronic file has the correct association, as with unique identifier, name, images, and criminal history record.

AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM—1: An automated, minutiae-based identification system that may consist of two or more distinct databases comprising two-finger identification records and ten-finger latent cognizant records (records of individuals more likely to be found at crime scenes, for example, burglars). 2: A computer-based system for reading, cataloguing, searching, matching, and storing fingerprints and related data. (ANSI/IAI) 3: A generic term for a fingerprint matching, storage, and retrieval system. (SWGFAST 2011)

AXIS—One of two intersecting lines superimposed on a displayed fingerprint image, used as a reference point to indicate orientation in a side-by-side comparison.

BENCHMARK TESTING—Standardized testing of a device or software to evaluate performance against some standard.

BIFURCATION—1: A point on a finger image where the friction ridge divides into two ridges. 2: The point at which one friction ridge divides into two friction ridges. (SWGFAST 2011)

CANDIDATE— 1: A master file record selected as a possible match to a current minutiae record, which results from either an automated name search or an automated (fingerprint) technical (AFIS) search. 2: A selection made by AFIS as a result of a search inquiry. (ANSI/IAI)

CANDIDATE LIST—The list of potential mates listed in descending order of their matching scores as determined by the matching process within the fingerprint minutiae matcher. A candidate list can also be produced by an Interstate Identification Index automated subject search. (ANSI/IAI)

CARD SCAN—1: An electronic scanning method of transmitting inked fingerprint impressions that meet local standards and the Federal Bureau of Investigation's image quality specifications and that are suitable for Store and Forward processing. 2: Electronic recording of friction ridge impressions (fingers and/or palms) from fingerprint cards, palm print cards, etc.; sometimes referred to as dead-scan or flat-bed scanner. (SWGFAST)

CHARGED-COUPLED DEVICE—1: An electronic chip capture device used in optical recording devices to convert light into electrical current. AFIS applications include digital cameras, card scans, Livescan, and other imaging equipment that captures fingerprint images on a chip. 2: An electronic chip capture device used in optical recording instruments that converts light energy into electrical current, e.g., the chip in a digital camera or scanner for capturing friction ridge impressions. (SWGFAST 2002)

COMPUTERIZED CASE HISTORY or **COMPUTERIZED CRIMINAL HISTORY**—Online case history information management system that lists all the criminal and non-criminal events that the identification agency is authorized to release to an inquiring agency; also referred to as the Rapsheet.

CRIMINAL JUSTICE INFORMATION SERVICES—A division of the Federal Bureau of Investigation.

CERTIFIED LATENT PRINT EXAMINER—A latent print examiner certified by the Latent Print Certification Board of the International Association for Identification.

CODER—Term for hardware, software, or both used to detect minutiae in a fingerprint image.

COMPARISON—1: The process of evaluating fingerprint images to be classified and/or identified for proper identification per user request. 2: The second step of the ACE-V method. 3: The observation of two or more impressions to determine the existence of discrepancies, dissimilarities, or similarities. (SWGFAST 2009)

COMPRESSION RATIO—Ratio of original file size as compared to the compressed file size. For AFIS, a 15:1 ratio is most often used.

CONCLUSION—Determination made during the Evaluation stage of ACE-V, including identification, inconclusive, or exclusion.

CONSOLIDATION—1: The merger of two or more records that are filed under more than one Federal Bureau of Investigation Number or identification number when it is determined that all pertain to one subject.

CORE—1: A well-defined center or focal point of a fingerprint image. 2: The approximate center or focal point of a friction ridge image (SWGFAST 2011). 3: A specific formation within a fingerprint pattern, defined by classification systems such as Henry.

CONTROL TERMINAL AGENCY—A state or territorial criminal justice agency on the National Crime Information Center system providing statewide or equivalent service to its criminal justice users. There is only one Control Terminal Agency per state or territory, and each operates under the supervision of a terminal agency coordinator.

DATABASE—A collection of data of a particular type, organized for efficient storage and retrieval (e.g., fingerprint minutiae data, fingerprint image data, or mugshot image data).

DELTA—That point on a ridge of a fingerprint image at or nearest to the point of divergence of two type lines and located at or directly in front of the point of divergence; also known as a tri-radius. (SWGFAST 2011)

DIGITAL IMAGE RETRIEVAL SYSTEM—An AFIS subsystem that contains the electronic fingerprint images.

DOWN SAMPLING—Process of representing an image with a smaller number of samples; may also be referred to as sub-sampling.

ELECTRONIC BIOMETRIC TRANSMISSON SPECIFICATON—A standard published by the Federal Bureau of Investigation for electronically encoding and transmitting biographic, biometric, and disposition information between federal, state, and local users and the Federal Bureau of Investigation, which specifies file, record content, format, and data codes.

ELECTRONIC FINGERPRINT TRANSMISSION SPECIFICATION (EFTS)—A standard published by the Federal Bureau of Investigation for electronically encoding and transmitting fingerprint images and identification and arrest data between federal, state and local users and the Federal Bureau of Investigation, which specifies file, record content, format, and data codes.

ELECTRONIC TEN-PRINT SUBMISSION—An electronic submission that originates at a Livescan booking terminal or card scanner at either the federal, state, or local level and is transmitted via the Criminal Justice Information Services wide area network to the Integrated Automated Fingerprint Identification System for processing. This type of electronic transaction contains fingerprint images and personal descriptor data. Processing of the transaction, including image comparison and the conclusion, is performed by Federal Bureau of Investigation personnel.

ELIMINATION FINGERPRINTS—1: Fingerprint images taken from persons with legitimate access to evidence under examination for latent fingerprint. 2: Exemplars of friction ridge skin detail of persons known to have had legitimate access to an object or location. (SWGFAST 2011)

ENCODING—AFIS process used to record minutiae.

ERRONEOUS EXCLUSION—The incorrect determination that two areas of friction ridge impressions did not originate from the same source. (SWGFAST 2011)

ERRONEOUS INDIVIDUALIZATION—The incorrect determination that two areas of friction ridge impressions originated from the same source. (SWGFAST 2011)

EURODAC—An AFIS formed by the European Union to track asylum seekers who apply for benefits.

EVALUATION—1: A determination by a latent print examiner about whether two impressions were made by the same source or different sources or if the information is inconclusive. 2: The third step in the ACE-V process.

EXCLUSION—The determination by an examiner that there is sufficient quality and quantity of detail in disagreement to conclude that two areas of friction ridge impressions did not originate from the same source. (SWGFAST 20111)

EXEMPLAR—1: An impression or image of friction ridge skin purposely collected with the knowledge of the subject. 2: The prints of an individual associated with a known or claimed identity deliberately recorded electronically, by ink, or by another medium (also known as known prints). (SWGFAST 2011)

EXPUNGEMENT—The process of either fully or partially purging data from a subject's record in the subject criminal history file. It results in the removal of all charges associated with the arrest covered by expungement while retaining the date of arrest and submitting originating agency identifier. Expungement requests are submitted by arrest or judicial agencies when an individual has been exonerated after initial arrest or released without charge and recorded as “detention only” or when so ordered by a court of appropriate jurisdiction.

FALSE CANDIDATE—A candidate selected by an AFIS search as a possible match, which is subsequently determined not identical.

FEATURES EXTRACTION—The system capability to identify from a scanned fingerprint digital image separately definable attributes, which may be discretely stored and used to classify and uniquely identify that fingerprint.

FEDERAL BUREAU OF INVESTIGATION NUMBER—A unique identifying number assigned by the Federal Bureau of Investigation to a subject of a fingerprint record of arrest who has not been identified as a previous offender in a search of the files.

FINGERPRINT—An impression of the friction ridges of all or any part of the finger. (SWGFAST 2011)
FINGERPRINT CHARACTERISTICS—Any aspects of fingerprints that can uniquely identify them.

FINGERPRINT CLASSIFICATION—1: A method for describing the common pattern fingerprint characteristics (e.g., pattern types or ridge counts) for the purpose of subdividing a fingerprint file into “classes” or groups having the same general characteristics so as to reduce the amount of the file needed to be searched to locate the mate (within the Integrated Automated Fingerprint Identification System, this may involve either Henry classification or pattern-level classification). 2: Grouping fingerprints according to shape and size for the purpose of filing and retrieving.

FINGERPRINT FEATURES—Unique physical characteristics of a fingerprint that are used to perform automated fingerprint searches.

FINGERPRINT FEATURES MASTER FILE—The set of all records on which fingerprint feature data exists.

FINGERPRINT IMAGE—A representative two-dimensional reproduction of the ridge detail of a fingerprint.

FINGERPRINT MATCHER SCORE—An AFIS-generated numerical score that indicates the approximate relationship between a latent print and an exemplar.

FINGERPRINT MINUTIAE—Unique identifying characteristics of fingerprints (e.g., beginning and ending points of ridges).

FINGERPRINT MINUTIAE MATCHER—The matching subsystem equipment that compares the minutiae data-based features of a search print with fileprints and selects the fileprint that comes closest to matching the search print. It will also perform a Minutiae Verification Match.

FINGERPRINT MINUTIAE MATCHER ACCURACY—1: A measure of the matcher subsystem's ability either to identify the correct candidate as a result of the matching process or to report that no candidate is selected if the mate is not in the fileprint database being searched. 2: The closeness of agreement between the matcher subsystem's generated representation of a fingerprint compared with the fingerprint it represents.

FINGERPRINT MINUTIAE MATCHER RELIABILITY—1: The probability that the mating fingerprint will be selected as the primary candidate by the matcher subsystem if that mate is in the fileprints being searched or that no candidate will be selected if the mate is not in the fileprints being searched. 2: The probability that an entity will perform its intended functions for a specified interval under stated conditions.

FINGERPRINT MINUTIAE MATCHER SELECTIVITY—The function of selecting the candidate, both correct and incorrect, and its relationship to other close candidates based upon minutiae scoring algorithms within the matcher subsystem.

FINGERPRINT PLAIN IMPRESSIONS—Fingerprint impressions taken by simultaneously capturing all of the fingers of each hand and then the thumbs without rolling, using a pressed or flat impression. See also, *plain, touch, or flat impression*.

FINGERPRINT REPOSITORY—A term for the AFIS/Federal Bureau of Investigation capability to store fingerprint characteristics data and perform database-like functions, such as storage retrieval, search, and update. The AFIS/Federal Bureau of Investigation Segment has at least three subcategories of repository:

(1) The *Federal Bureau of Investigation Criminal Repository* contains one entry for each subject meeting retention criteria. The data included are extracted from criminal ten-print submissions. At a minimum, the Federal Bureau of Investigation Criminal Repository contains fingerprint characteristics for all ten fingers.

(2) The *Unsolved Latent Repository* contains single latent fingerprints not identified to any subject in the criminal fingerprint repository. It is used to provide leads for unsolved criminal cases.

(3) The *Special Repositories* have separately defined uses and data. Each has its own sponsor who controls its use. The data in each repository may be used for either ten-print and latent fingerprint searching or for specially defined fingerprint searching.

FINGERPRINT ROLLED IMPRESSIONS—The impressions created by individually rolling each inked finger from side to side in order to obtain all available ridge detail. See also, *inked rolled print*.

FAST FOURIER TRANSFER ALGORITHM—An algorithm used in digital image processing to decompose and compose a signal.

FLATS—Fingerprint plain impressions. See also, *plain, touch, or flat impression.*

FRICTION RIDGE—1: The ridge-shaped skin on a finger or palm surface that makes contact with an object. 2: A raised portion of the epidermis on the palmar or plantar skin, consisting of one or more connected ridge units. (SWGFAST 2011)

GRAY-SCALE IMAGE—An image using more than two radiometric values, i.e., 256 shades of gray in an 8-bit image. Not a strictly black/white image.

GROUP IV FAX—A facsimile transmitted fingerprint card suitable for identification processing.

HENRY CLASSIFICATION—An alphanumeric system of fingerprint classification named after Sir Edward Richard Henry used for filing, searching, and retrieving ten-print records. (SWGFAST 2011)

HIT RESPONSE or **HIT ON FINGERPRINT SEARCH**—An identification of minutiae-based data of a fingerprint image with minutiae-based data from another fingerprint image as being a mate for the finger of the same person.

INTEGRATED AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM—The Federal Bureau of Investigation's national AFIS. (SWGFAST 2011) IAFIS provides: (a) repository maintenance services, such as receipt, storage, and retrieval; (b) powerful search functions that attempt to match submitted fingerprints with fingerprints in the repository; and (c) fingerprint characteristics processing capability to derive unique aspects of fingerprints for storage and matching.

INTERNATIONAL ASSOCIATION FOR IDENTIFICATION—Professional association whose members are engaged in forensic identification, investigation, and scientific examination of physical evidence.

IDENTIFICATION—1: The positive match of a current ten-print or latent fingerprint card to a prior fingerprint card stored in the fingerprint files, made on a comparison of one set of fingerprints to another. 2: In some forensic disciplines, the similarity of class characteristics. (SWGFAST 2011) See also, *individualization*.

INDIVIDUALIZATION—The determination by an examiner that there is sufficient quality and quantity of detail in agreement to conclude that two friction ridge impressions originated from the same source. (SWGFAST 2011)

IMAGE—Processed or stored fingerprint images from a ten-print card or latent lift.

INKED ROLLED PRINT—An inked fingerprint impression taken by physically rolling the inked finger from side to side (nail to nail) on the fingerprint card stock. See also, *rolled impression*.

INTEROPERABILITY—The ability of two or more AFIS networks, systems, devices, applications or components to exchange information between them and to use the information so exchanged correctly and with minimal loss of accuracy.

INTERPOL—Originally the International Police Commission, established in 1923 with the first headquarters in Vienna, Austria. With the General Secretariat now in Lyon, France, Interpol focuses on international crimes that threaten public safety, especially those involving terrorism, criminal organizations, drugs, finances and technology, and trafficking in human beings, and provides fugitive investigative support.

INTERSTATE IDENTIFICATION INDEX—A national network for the exchange of criminal history records, which includes elements of participating state systems, the National Crime Information Center System, the Identification Automated Services of the Federal Bureau of Investigation, the National Law Enforcement Telecommunications Network, and the U.S. Postal Service, among other systems.

IMAGE QUALITY SPECIFICATION—Element of the Electronic Fingerprint Transmission Specification that has two components, Appendix F and Appendix G.

JOURNAL OF FORENSIC IDENTIFICATION—A publication of the International Association for Identification.

JPEG—1: An acronym for the Joint Photographic Experts Group. 2: A compression file format with the ".jpg" file extension, most of which use lossy compression.

LATENT COGNIZANT DATABASE—Fingerprint features records of all ten fingers of a subset of criminals in the ten-print database, used for matching latent fingerprint submissions, which may be partial fingerprints. Includes fingerprint data from certain crime categories (e.g., bank robbery or terrorism).

LATENT PRINT—1: Transferred impression of friction ridge detail not readily visible. 2: Generic term used for unintentionally deposited friction ridge detail. (SWGFAST) 3. The reproduction of the friction ridges on an item that is touched when the ridges come in contact with any contaminant.

LATENT PRINT SUBMISSION—A submission to the Federal Bureau of Investigation or other agency that contains a latent fingerprint search request accompanied by the latent fingerprint information, either electronic or hardcopy.

LATENT PRINT LIFT—1: A reproduction of the friction ridge detail of a latent print. 2: An adhesive or other medium used to transfer a friction ridge impression from a substrate. (SWGFAST 2011)

LATENT PRINT SEARCH—A comparison of the fingerprint features extracted from a latent fingerprint with the fingerprint features contained in a fingerprint features file to determine whether a latent fingerprint has a potential mate on file within the AFIS repository.

LATENT PRINT SPECIALIST—Law enforcement agency employee who performs latent print processing.

LATENT PRINT SUBMISSION—One image and associated descriptor data received by latent processing services, which may be part of a case.

LAW ENFORCEMENT ONLINE—National, interactive communications system maintained by the Federal Bureau of Investigation exclusively for law enforcement.

LIGHTS OUT—An AFIS search without any human intervention at Verification.

LIVESCAN PRINT—A fingerprint image that is produced by scanning a live finger with Livescan technology.

LIVESCAN—An electronic method of taking and transmitting fingerprints without using ink, which produces fingerprint impressions of high quality to perform identification processing.

LOCAL MODE—Process by which a workstation can perform some function independent of AFIS (function may be limited to acquisition of new records).

LATENT/LATENT SEARCH—A search of a latent print against other latent prints, which are usually stored in the Unsolved Latent File, and which has the potential to link crimes committed by same person, even though that person is as yet unidentified. Also referred to as a latent/unsolved latent search.

LATENT/TEN-PRINT IDENTIFICATION DATABASE SEARCH—A search of a latent print against the ten-print identification database.

LATENT/TEN-PRINT LATENT COGNIZANT SEARCH—A search of a latent print against the ten-print latent cognizant (ten-finger) database.

LATENT/UNSOLVED LATENT SEARCH—See latent/latent search.

MASTER NAME INDEX—A subject identification index maintained by criminal history record repositories that includes names and other identifiers for each person with a record in the database.

MATCH—Condition of retrieving a file subject that, because of matcher score, falls within selection criteria for the probability of a mate to a search suspect.

MATCHER—An AFIS component that compares the minutiae database features of a search print with fileprints and selects the fileprint that comes closest to matching the search print.

MATCHER ACCURACY—A measure of the matcher subsystem's ability to place the correct mates as the selected candidate as a result of the matcher process, or a measure of the matcher subsystem's ability to select no candidate if the mate is not in the database.

MATCHER RELIABILITY—1: The probability that the mate fingerprint will be selected as the primary candidate by the matcher if it is in the file being searched, or that no candidate will be selected if the mate is not in the file being searched. 2: The probability that the matcher will function as intended for a specified interval under specific conditions.

MATCHING SCORE—The numerical result of comparing the minutiae data of two fingerprint digital representations.

MATE—1: A fingerprint that matches another impression from the same finger. 2: A fingerprint that is another impression from the same finger. (ANSI/IAI)

MINUTIAE—1: Friction ridge characteristics that are used to individualize the print and that occur at points where a single friction ridge deviates from an uninterrupted flow. Deviation may take the form of ending, dividing into two or more ridges, or immediately originating and terminating. (ANSI/IAI) 2: Events along a ridge path, including bifurcations, ending ridges, and dots (also known as Galton details). (SWGFAST)

MINUTIAE DATA—The data representing the relative position, orientation, and in some cases, the relationship and/or types of the minutiae in a fingerprint image. (ANSI/IAI)

MINUTIAE SEARCHING—The process of comparing the search print against the fileprints by scoring the match of minutiae data in the prints and ranking the scores either to produce one candidate with the highest score who is the potentially identical mate for the same finger, or to produce no candidate when the potentially identical print does not exist within the fileprint database.

MINUTIAE VERIFICATION MATCH—The process of comparing minutiae data from a subject's previously entered single fileprint with minutiae data from a single incoming search print and, thereafter, comparing the resultant match score with a threshold to determine if the prints are potential mates.

MATCHER QUALITY INDEX—Value representing the sum of the "equivalent number of minutiae" for fingers 2 and 7 (generally the search fingers). The index is a complex metric that weights the actual minutiae count using local image quality and the number of neighbors in computation. On the average fingerprint, the Integrated Automated Fingerprint Identification System produces about 88 minutiae, and the average value for the equivalent number of minutiae is about 56. Images with higher matcher quality index values are more likely to be successfully matched by the Integrated Automated Fingerprint Identification System.

NAIL-TO-NAIL ROLL—See *rolled impression*.

NAME SEARCH—A routinely searched database program/file that can yield the State Identification Number of individuals in the database if they have used the same descriptive information for a prior event.

NATIONAL CONSORTIUM FOR JUSTICE INFORMATION AND STATISTICS—See *SEARCH*.

NATIONAL CRIME INFORMATION CENTER—A computer system established in 1967 to provide criminal record history, fugitives, missing persons, and stolen property information to local, state, and federal agencies. Succeeded by National Crime Information Center 2000.

NATIONAL CRIME INFORMATION CENTER 2000—Successor to National Crime Information Center, a network that provides information to local, state, and federal criminal justice agencies through computer terminals and mobile applications.

NATIONAL FINGERPRINT FILE—A component of the Interstate Identification Index that decentralizes interstate exchange of criminal history records by containing fingerprints from all federal offenders but only one first-arrest set of fingerprints from select state offenders with other biometric data, requiring states to maintain the criminal history.

NATIONAL INCIDENT-BASED REPORTING SYSTEM—An outgrowth of the uniform crime report and a byproduct of the state and local incident-based reporting systems, which collects specific crime information on 22 offense categories consisting of 46 specific crimes collectively called Group A offenses, including data on victims, offenders, and circumstances. For the 11 offensive categories known as Group B, only arrest information is captured.

NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM—A non-fingerprint-based search database accessible through the Internet and required before purchasing a firearm. Federal Firearms Licensees record descriptive information on the Bureau of Alcohol, Tobacco, Firearms and Explosives' Form 4473.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY—Formerly known as the National Bureau of Standards, this division of the U.S. Department of Commerce ensures standardization in non-defense government agencies.

NEXT GENERATION IDENTIFICATION—Program to advance the Federal Bureau of Investigation's biometric identification services, providing an incremental replacement of current Integrated Automated Fingerprint Identification System technical capabilities, while introducing new functionality across a multi-year timeframe.

NLETS—An outgrowth of Law Enforcement Teletype System, Nlets was incorporated in 1970 as a not-for-profit organization. Nlets provides an international, computer-based message system that links local, state, and federal criminal justice agencies for information exchange and provides information services support for justice-related applications by supporting data communications links to state networks using commercial relay services.

NON-IDENTIFICATION—A determination that two fingerprints do not belong to a particular person or that no mate is found as the result of a fingerprint comparison.

ORIGINATING AGENCY IDENTIFIER—An identification number assigned by the National Crime Information Center or the Integrated Automated Fingerprint Identification System to each agency that may submit information into, or receive information from, either system. The format of this number varies from agency to agency, except that the first two characters always designate the state, territory, province, or country of the contributor.

PALM PRINT—1: An inked and rolled or Livescan of the palms of both hands. May also include the side of the hand referred to as the writers palm. 2: An impression of the friction ridges of all or any part of the palmar surface of the hand. (SWGFAST 2011)

PATTERN CLASSIFICATION—Characterization of a fingerprint as containing one of seven fingerprint patterns: arch, tented arch, right-slant loop, left-slant loop, whorl, amputation, or scar. The Integrated Automated Fingerprint Identification System will provide for both pattern-level and Henry classifications.

PROCESS CONTROL NUMBER—A temporary identifier of a ten-print record until matching State Identification Number is found (by locating a match in the database) or a new State Identification Number is assigned (if there is no match on the database).

PEAK MINUTE—A minute during which a system must process a statistically significantly greater number of user support functions than it is required to process during an average minute.

PIXEL—The smallest element of a picture that is digitized as an entity. (ANSI/IAI)

PLAIN, TOUCH, OR FLAT IMPRESSION—Impressions of all four fingers from each hand, taken simultaneously, and of the thumbs, taken without rolling, which appear at the bottom of the fingerprint card and serve to verify the proper sequence of the rolled (or Livescan) impressions and to provide additional ridge detail for comparison. (ANSI/IAI)

PROTOTYPE—A simulation of a program, report, menu, or system.

QUALITY CONTROL—1: Editing of fingerprint minutiae to improve accuracy for identification, automatically determined for ten-prints. 2: Measures that are taken to ensure that an acceptable level of system performance is maintained. (ANSI/IAI)

RADIOMETRIC RESOLUTION—Number of intensity levels (i.e., shades of gray or color values) in a digital image.

RELAUNCH—Searching a latent print case after the initial latent/ten-print latent cognizant database search using different search parameters while maintaining the same case identifiers and images.

RELIABILITY—The probability that the mating fingerprint will be a candidate if the mate is in the file being searched.

REMOTE TEN-PRINT FINGERPRINT FEATURE SEARCH (NATIVE MODE)—A search request transmitted to the Federal Bureau of Investigation originating outside the Identification Tasking and Networking workstations containing fingerprint characteristics derived by an AFIS in a similar manner to those derived by the Integrated Automated Fingerprint Identification System and containing the necessary fingerprint classifications and other data. The search request is performed automatically by the Integrated Automated Fingerprint Identification System without human involvement.

REVERSE SEARCH—See *ten-print/unsolved latent search*.

REMOTE FINGERPRINT EDITING SOFTWARE—Software package from the Federal bureau of Investigation to perform remote searches on the Integrated Automated Fingerprint Identification System, which supports remote Integrated Automated Fingerprint Identification System transactions including image- and features-based searches for latent and ten-print applications. Succeeded by Universal Latent Workstation.

ROLLED IMPRESSION—Fingerprint impressions created by individually rolling each finger from side to side (nail to nail) to obtain all available friction ridge detail. The images appear in the individual print boxes on the ten-print card.

SCANNER—Capture device to create a digital image. New scanners that connect to the Federal Bureau of Investigation must meet the standards outlined in Appendix F of the *Electronic Biometric Transmission Specification*.

SEARCH SELECTIVITY—The total number of incorrect candidates divided by the total number of searches conducted during the time period; that is, it is the number of incorrect candidates, averaged over time periods, produced for comparison per search at the operating point at which search reliability is measured.

SEARCH or **THE NATIONAL CONSORTIUM FOR JUSTICE INFORMATION AND STATISTICS**—A nonprofit membership organization dedicated to better criminal justice information management, effective identification technology, and responsible law and policy.

SEGMENT—One of the constituent parts into which an automated system may be logically divided.

STATE IDENTIFICATION NUMBER—Number assigned to each individual on a state file.

SUBJECT MATTER EXPERT—Person who exhibits the highest level of expertise in performing a specialized job, task, or skill.

STATEMENT OF WORK—Describes the tasks and responsibilities for a project.

SPATIAL RESOLUTION—Relationship of the individual pixels to the size of the actual area represented.

SPECTRAL RESOLUTION—Color bands of light detected during image acquisition.

STATE-OF-THE-ART TECHNOLOGY—The highest level of development of a device or technique achieved at any particular time.

STORE AND FORWARD—A system capable of electronically receiving and processing fingerprint cards at the state and then sending the fingerprints electronically into AFIS and to the Federal Bureau of Investigation.

SUBJECT SEARCH—A search, using biographical and/or physical data, to identify a list of candidates having records that match the descriptors specified; can be based upon name, gender, date of birth, Federal Bureau of Investigation Number, State Identification Number, Social Security Number, or other biographical or physical data (e.g., height, weight, age) or combinations of these characteristics.

SCIENTIFIC WORKING GROUP ON FRICTION RIDGE ANALYSIS, STUDY AND TECHNOLOGY—A group of local, state, and federal law enforcement officials and members of the community who establish guidelines for the development and enhancement of friction ridge examiners' knowledge, skills, abilities, methods, and protocols; who establish guidelines for quality assurance; and who cooperate with national and international standards organizations to disseminate their findings.

TERMINAL AGENCY COORDINATOR—Individual in the control terminal agency who is responsible for monitoring system use, enforcing system discipline, and ensuring National crime Information Center operating procedures are followed.

TECHNICAL SEARCH—Using AFIS, a minutiae-based fingerprint search, usually with the index fingerprints of the ten-print record but sometimes with the thumbs or a combination of index fingers and thumbs.

TEN-PRINT—A fingerprint card (or fingerprint card equivalent) containing rolled and plain impressions from the ten fingers of an individual. The standard format contains 14 impressions: one rolled fingerprint impression of each finger, plain fingerprint impressions of each thumb, and plain impressions of the four fingers of each hand simultaneously.

TEN-PRINT CARD SUBMISSION—A fingerprint card submitted to the Federal Bureau of Investigation by mail, facsimile, or other electronic method for the purpose of identification and possible incorporation into the Federal Bureau of Investigation's Fingerprint Repository.

TEN-PRINT IMAGE SEARCHES—An electronic transaction submitted to the Federal Bureau of Investigation, which contains fingerprint images, classification information as required by the Integrated Automated Fingerprint Identification System, or remotely extracted fingerprint characteristics. The subsequent search will be conducted automatically with no additional manual editing or processing. If candidates are identified, the candidates' Federal Bureau of Investigation Numbers are returned to the transmitting agency along with fingerprint images from the highest scoring candidates.

TAGGED IMAGE FILE FORMAT—An image file format with the ".tif" file extension, which can be either lossless or lossy.

TEN-PRINT/TEN-PRINT IDENTIFICATION DATABASE SEARCH—Search of a ten-print record against the records in the ten-print identification database.

TEN-PRINT/UNSOLVED LATENT SEARCH—Search of a new ten-print record against the records in the unsolved latent file in expectation that the owner of the latent print did not have a record in the ten-print database at the time of the latent/ten-print search. Also referred to as a reverse search.

TEN-PRINT IDENTIFICATION DATABASE—Database consisting of two finger images, usually the index fingers but sometimes the thumbs.

TEN-PRINT LATENT COGNIZANT DATABASE—Database consisting of all ten finger images, which may be a subset of the ten-print identification database.

TRANSPOSITION—Incorrect position of hands on the ten-print card (e.g., images of the right hand appear in boxes for the left hand). In the past, identification staff would visually inspect the rolled impressions against the plain impressions for consistency. Livescan software for extraction and comparison reduce this burden on digitally retrieved images.

TECHNOLOGY WITHOUT AN IMPORTANT NAME—Image acquisition and output protocol commonly used between computers, printers, and image capture devices.

UNIFORM CRIME REPORT—Voluntary reporting of crimes (including murder, non-negligent manslaughter, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson) to the Federal Bureau of Investigation's Criminal Justice information Services Division.

UNSOLVED LATENT/UNSOLVED LATENT SEARCH—A search of the unsolved latent print file using another unsolved latent print to determine if latent images from the same subject are on file even if the subject remains unknown. May be used to determine a serial offender and for sharing information with another agency.

UNIVERSAL LATENT WORKSTATION—Software program developed by the Federal Bureau of Investigation's Criminal Justice information Services Division that, when installed on a commercial off-the-shelf computer, allows the operator to create a native feature set for AFIS vendors by which the Integrated Automated Fingerprint Identification System can receive and search an ANSI/NIST-formatted record.

UPGRADE—Introduction of new software and/or hardware into an existing system. The upgrade may be to fix certain known problems unique to one AFIS customer, to fix known problems applicable to all customers, to provide an improvement to the AFIS system not related to a problem, or to enable a move to a new platform (such as from Microsoft® Windows® to Linux, or Windows® 98 to Windows® XP). The upgrade may require extensive on-site testing prior to installation on the live system.

VALIDATION—Process of comparing data or images against a previously verified set of data; a double check of the verification that confirms the accuracy of a system prior to use.

VERIFICATION—1: Process of visually comparing a search fingerprint with a candidate fingerprint to determine if there is a match after another latent print examiner has already reached a conclusion. 2: The fourth and final step in the ACE-V process.

WIDE AREA NETWORK—A network that interconnects geographical entities, such as cities and states, generally covering a distance of 50 miles or greater.

WAVELET SCALAR QUANTIZATION—A lossy compression algorithm used to reduce finger or palm print images size.

ACRONYM LIST

ABIS—Automated Biometric Identification System

AFIS—Automated Fingerprint Identification System

ANSI—American National Standards Institute

APB—Advisory Policy Board

ARG—Attributed Relational Graph

ASCII—American Standard Code for Information Interchange

ATB—Automated Fingerprint Identification System Test Bed

BCI&I—Bureau of Criminal Identification and Investigation

BoM—Bill of Material

CAN—Criminal Ten-Print Submission (No Answer Necessary)

CAR—Criminal Ten-Print Submission (Answer Required)

CARC—Criminal Ten-Print Card Scanning Service Submission (Answer Required)

CAXI—Core and Axis Independent

CCD—Charged-Coupled Device

CCH—Computerized Case History or Computerized Criminal History

CJIS—Criminal Justice Information Services

CLPE—Certified Latent Print Examiner

CMF—Criminal Master File

CNAC—Criminal Ten-Print Card Scanning Service Submission (No Answer Necessary)

CODIS—Combined DNA Index System

CONOPS—Concept of Operations

COTS—Commercial Off-the-Shelf

CSS—Card Scanning Service

CTA—Control Terminal Agency

DCJS—New York State Division of Criminal Justice Services

DEU—Unknown Deceased

DIRS—Digital Image Retrieval System

DMS—Data Management System

DNA—Deoxyribonucleic Acid

DPS—Department of Public Safety

EBTS—Electronic Biometric Transmission Specification

EFCON—Electronic Fingerprint Converter

EFTS—Electronic Fingerprint Transmission Specification

EFS—Extended Feature Set

FANC—Federal Applicant – No Charge Federal Agency Name Check

FAR—False Acceptance Rate

FAT—Factory Acceptance Test

FAUF—Federal Applicant User Fee

FBI—Federal Bureau of Investigation

FFT—Fast Fourier Transfer

FIC—Fingerprint Image Comparison

FIMF—Fingerprint Image Master File

FNCC—Federal Applicant Card Scanning Service Submission (No Charge)
FNU—Federal Bureau of Investigation Number
FPF—Focal Point Filtering
FPT—Fast Fourier Number
FpVTE—Fingerprint Vendor Technology Evaluation
FUFC—Federal Applicant Card Scanning Service Submission (User Fee)
GFE—Government-Furnished Equipment
IAFIS—Integrated Automated Fingerprint Identification System
IAI—International Association for Identification
IBR—Incident-Based Reporting
ICD—Interface Control Document
IDAS—Identification Automated Services of the Federal Bureau of Investigation
III—Interstate Identification Index
IISS—Identification and Investigative Services Section of Criminal Justice Information Services Division
IMAP—Internal Miscellaneous Applicant Civil
IQS—Image Quality Specification
IRC—Indeterminate Ridge Count
IT—Information Technology
ITL—Information Technology Laboratory
ITN—Identification Tasking and Networking
JFI—Journal of Forensic Identification
JPEG—Joint Photographic Experts Group
LDIS—Local DNA Index System
LEIF—Law Enforcement Interconnecting Facilities
LEO—Law Enforcement Online
LETS—Law Enforcement Teletype System
LFFS—Latent Fingerprint Feature Search
LFIS—Latent Fingerprint Image Search
LITS—Latent Interoperability Transmission Standard
LT—Latent Print
LT-ARG—Latent-Attributed Relational Graph
MAP—Miscellaneous Applicant Civil
MAPC—Miscellaneous Applicant Card Scanning Service Submission (No Charge)
MCAXI—Modular Core and Axis Independent
MCS—Minutiae Comparison Standard
MOU—Memorandum of Understanding
MPR—Missing Person
MQI—Matcher Quality Index
N-FACS—National Fingerprint-Based Applicant Check Study
NCIC—National Crime Information Center
NCIC 2000—National Crime Information Center 2000
NDIS—National DNA Index System
NFF—National Fingerprint File

NFFC—Non-Federal Applicant Card Scanning Service Submission (User Fee)
NFUF—Non-Federal Applicant User Fee
NGI—Next Generation Identification
NIBRS—National Incident-Based Reporting System
NICS—National Instant Criminal Background Check System
NIJ—National Institute of Justice
NIST—National Institute of Standards and Technology
NOE—Non-Operational Environment
NPS—National Police Services
NSOR—National Sex Offender Registry
NYSIIS—New York State Identification and Intelligence System
O&M—Operations and Maintenance
ODRC—Ohio Department of Rehabilitation and Correction
OE—Operational Environment
OLES—Law Enforcement Standards Office
ORI—Originating Agency Identifier
PC/RC—Pattern Class/Ridge Count
PCN—Process Control Number
POC—Point of Contact
PPI—Pixels per Inch
PSS—Public Safety Strategy
QC—Quality Control
RFES—Remote Fingerprint Editing Software
RFI—Request for Information
RFP—Request for Proposals
RRI—Repository Retrieval Index
SAN—Storage Area Network
SAT—Site Acceptance Test
SDIS—State DNA Index System
SID—State Identification
SME—Subject Matter Expert
SMT—Scars, Marks, and Tattoos
SoS—System-of-Systems
SOW—Statement of Work
SP/CR—System Problem/Change Report
SSN—Social Security Number
SWGFAST—Scientific Working Group on Friction Ridge Analysis, Study and Technology
TAC—Terminal Agency Coordinator
TAR—True Acceptance Rate
TBD—To Be Determined
TIFF—Tagged Image File Format
TOT—Type of Transaction
TP—Ten-Print Record
TP-CMF-CAXI—Ten-Print Criminal Master File Core and Axis Independent

TP-ARG—Ten-Print-Attributed Relational Graph
TPid—Ten-Print Identification Database
TPIS—Ten-Print Image Search
TPlc—Ten-Print Latent Cognizant Database
TWAIN—Technology Without an Important Name
UCR—Uniform Crime Report
UL—Unsolved Latent
ULF—Unsolved Latent File
ULW—Universal Latent Workstation
UP—Unsolved Palm
USSS—United States Secret Service
VPN—Virtual Private Network
WAN—Wide Area Network
WDS—Workflow Distribution Server
WIN—Western Identification Network
WSQ—Wavelet Scalar Quantization