NIST Special Publication 1156

Writing Guidelines to Develop a Memorandum of Understanding for Interoperable Automated Fingerprint Identification Systems

Susan Ballou
Anthony Clay
Joi Dickerson
Mike Garris
Peter T. Higgins
Janet Hoin
Lisa Jackson
Peter Komarinski
Mike Lesko
Joe Morrissey
Leo Norton
Beth Owens
Joe Polski
Melissa Taylor

http://dx.doi.org/10.6028/NIST.SP.1156

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1156

Writing Guidelines to Develop a Memorandum of Understanding for Interoperable Automated Fingerprint Identification Systems

Susan Ballou
Melissa Taylor
Law Enforcement Standards Office
Office of Special Programs

Anthony Clay
United States Secret Service

Joi Dickerson
Culver City, California, Police Department

Mike Garris
Information Technology Laboratory

Peter T. Higgins
Higgins & Associates, International
Washington, DC

Janet Hoin
Joe Morrissey
New York State Division of Criminal Justice Services

Lisa Jackson
Santa Monica, California, Police Department

Peter Komarinski
Komarinski and Associates

Mike Lesko
Texas Department of Public Safety

Leo Norton
Los Angeles County, California, Sheriff's Department

Beth Owens
Franklin County, Ohio, Sheriff's Office

Joe Polski
Retired
International Association for Identification

http://dx.doi.org/10.6028/NIST.SP.1156

May 2013

U.S. Department of Commerce
Rebecca Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Special Publication 1156
Natl. Inst. Stand. Technol. Spec. Publ. 1156, 43 pages (May 2013)
http://dx.doi.org/10.6028/NIST.SP.1156
CODEN: NSPUE2

Writing Guidelines to Develop a Memorandum of Understanding for Interoperable Automated Fingerprint Identification Systems

Latent Print AFIS Interoperability Working Group

Law Enforcement Standards Office (OLES)

Helping law enforcement, corrections, criminal justice, and public safety agencies ensure that the equipment they purchase and the technologies they use are safe, dependable, and effective.

A division of

National Institute of Standards and Technology

Enter Once, Search Many

Contents

FOREWORD....1
HOW TO USE THIS GUIDE....4
GETTING STARTED....6
Workflow....6
1. Introduction Section....7
2. Purpose Section....8
3. Scope Section....9
4. Policy Section....13
5. Oversight Section....14
6. Compliance Section....15
7. Updates to the MOU Section....15
8. Financial Considerations Section....16
ATTACHMENT I: Template for a Latent Print Processing Agreement between the Hosting Agency and the Requesting Agency....A1-1
ATTACHMENT II: Operational Responsibilities Template....A2-1
ATTACHMENT III: Automated Fingerprint/Biometric Identification System User Qualifications Guidelines Template....A3-1
ATTACHMENT IV: Abbreviation List....A4-1

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 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
Peter Komarinski	Komarinski and Associates
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 (Retired)
Melissa Taylor	National Institute of Standards and Technology

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; and
- ❑ 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 NIST OLES reference documents to help agencies achieve interoperability, located at http://www.nist.gov/oles/afis_interoperability.cfm.

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 the following sections:

- ❑ 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
- ❑ Attachment IV: Abbreviation List

This document does not address every issue that may arise between different agencies that 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, and
- ❑ vendors.

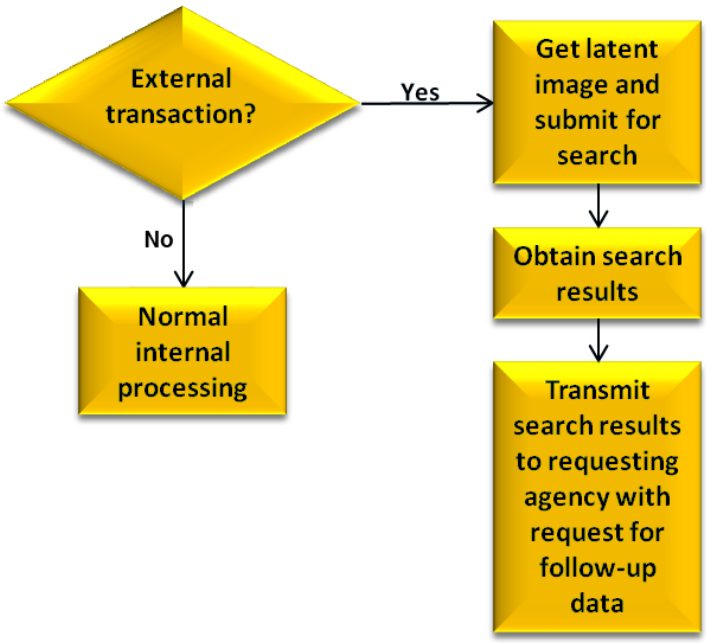
Workflow

It can prove helpful to develop a workflow document 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; and
- ❑ 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



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 *[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, or other]*.

Example Language

Agreement on transaction formats

Agencies will use the following standard transaction formats: *[selected from CJIS's Electronic Biometric Transmission Specification, American National Standards Institute/NIST, or the Latent Interoperability Transmission Specification 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; and 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; and 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; and 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; and 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:

- ❑ disclosure of protected information (personally identifiable information)
- ❑ breach of security of the system
- ❑ any misuse
- ❑ failure to abide by financial arrangements
- ❑ *[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 to which the member agencies have agreed. 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 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 revisions 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.** Member agencies agree on the coat per search 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]*.

Page intentionally left blank.

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 that 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; and
- ❑ confer as needed.

Responsibilities of the Requesting Agency

The Requesting Agency shall do the following:

- ❑ 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.
- ❑ 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; and
- ❑ 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 hours 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;
- ❑ ten-print to latent searches to *[insert #]* per day or *[insert #]* per week;
- ❑ latent palm to palm searches to *[insert #]* per day or *[insert #]* per week; and/or
- ❑ 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), including 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; and
- ❑ 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 do the following:

- ❑ 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 do the following:

- ❑ 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 is not 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; and
- ❑ provide additional information and/or training on any AFIS updates/changes.

Responsibilities of the Requesting Agency

The Requesting Agency shall

- ❑ coordinate AFIS-related training in conjunction with the manager at the Hosting Agency;
- ❑ suggest new AFIS training procedures as needed;
- ❑ provide training sessions to other Requesting Agency personnel and User Agency examiners subsequent to the Hosting Agency/Vendor-provided training session, which should include instruction on the Requesting Agency's AFIS procedures;
- ❑ conduct updates and refresher training as needed; and
- ❑ 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; and

- ❑ 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; and
- ❑ 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

Page intentionally left blank.

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 real 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 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:

Abbreviation List

ABBREVIATION LIST

AFIS—Automated Fingerprint Identification System
CJIS—Criminal Justice Information Services
FBI—Federal Bureau of Investigation
MOU—Memorandum of Understanding
NIJ—National Institute of Justice
NIST—National Institute of Standards and Technology
OLES—Law Enforcement Standards Office
POC—Point of Contact
UL—Unsolved Latent
ULF—Unsolved Latent File
UP—Unsolved Palm
WAN—Wide Area Network