United States
Department of Justice

U.S. Department of Justice's Global

Global Reference Architecture (GRA)

Information Sharing Enterprise Service-Level Agreement (SLA)

Version 1.1

April 2011

Global Infrastructure/Standards Working Group

This project was supported by Grant No. 2008-DD-BX-K520 awarded by the Bureau of Justice Assistance, Office of Justice Programs, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.

Table of Contents

As a part of Global's effort to support information sharing activities that span jurisdictional boundaries within and outside of criminal justice, the Justice Reference Architecture (JRA) has been rebranded to the Global Reference Architecture (GRA). This change will not introduce any significant technical modifications to the architecture but is rather intended to provide a more inclusive service-oriented model that will meet the broader needs of justice, public safety, homeland security, health and human services, and additional stakeholders. The GRA, therefore, is designed to be an information sharing architecture that will meet the needs of government at all levels and fulfill the need for improved collaboration across communities.

Acknowledgements

The **GLOBAL REFERENCE ARCHITECTURE** (GRA) was developed through a collaborative effort of the Global Justice Information Sharing Initiative (Global) and the U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA). GISWG would like to express its appreciation to BJA for its support and guidance in the development of GRA resources, such as this document. These resources provide invaluable assistance to local, state, regional, federal, and tribal entities toward the goal of improved information sharing.

Global aids its member organizations and the people they serve through a series of important initiatives. These include the facilitation of Global Working Groups. The Global Infrastructure/Standards Working Group (GISWG) is one of five Global Working Groups covering critical topics such as intelligence, privacy, security, outreach, and standards. GISWG consists of three committees—Management and Policy, Services Implementation, and Enterprise Architecture. Global would like to recognize the members of the GISWG Management and Policy Committee for their contributions to this resource:

Thomas Clarke, Ph.D., Chair
GISWG
National Center for State Courts

Mr. Dale Good, Chair
GISWG Management and Policy Committee
Judicial Council of California—Administrative Office of the Courts

Mr. Roger Banner
North Carolina Administrative Office of the Courts

Mr. Oded Galili
Minnesota Bureau of Criminal Apprehension

Mr. Mark Perbix
SEARCH, The National Consortium for Justice Information and Statistics

Ms. Christina Rogers
California Department of Justice

Mr. Joseph Wheeler
IJIS Institute

Mr. Robert Woolley
State of Utah

Document Conventions

In this document, use of a bold small-caps typeface, as in this **EXAMPLE**, indicates an important concept, term, or document defined or referenced either in the body of the text or section ***18. References and Documents*** of this document.

About This Document

Target Audience: This document is recommended for the person responsible for drafting a new SLA and/or reviewing and refining an existing agreement in an agency, department, company, or organization that offers or uses an information sharing service, particularly (but not limited to) within the Global Justice Information Sharing Enterprise (GJISE). In most cases, that will be a manager and/or legal counsel. Executive managers—those who ultimately sign the agreement—may also be interested in this resource, particularly if they play a role in the development or refinement of the SLA.

Purpose and Contents: The purpose of this document is to provide a sample Service-Level Agreement (SLA), in this case, for a fingerprint service to local, state, tribal, or federal justice and public safety agencies organized under a Statement of Participation or similar umbrella agreement. This document may be consulted as an example to facilitate the understanding of what is intended to be included in each SLA section. It provides an example of the expectations and obligations for those offering (**PROVIDER**) or using (**CONSUMER**) a specific information sharing service within the GJISE. This SLA is an extension of the governing **GJISE STATEMENT OF PARTICIPATION.**

Where this SLA example benefits from additional exposition, a "Commentary" section is included in call boxes within the associated section.

This resource is intended as a comprehensive, educational, and annotated SLA, specific to the fingerprint service. It should be noted that a companion document, a **SERVICE-LEVEL AGREEMENT TEMPLATE,** is under development. This template will be a complete, easily transferable and reusable "plug-and-play" solution: i.e., a hands-on tool to facilitate rapid creation of an SLA for any service.

Background: This SLA was developed by the GISWG Management and Policy (M&P) Committee as part of a suite of governance-related resources to facilitate justice information sharing. The resource was vetted by the GISWG leadership team—the Executive Architecture Committee—and approved by members of the U.S. DOJ's Global Advisory Committee as a recommendation to fellow justice practitioners and industry partners. This Global collection of governance resources includes the **GJISE STATEMENT OF PARTICIPATION,** developed by the same GISWG M&P Committee, which serves as the fundamental GRA services governance document; this SLA is meant to be used in conjunction with that initial document. The suite of products also includes policy guidelines associated with the **GLOBAL FEDERATED IDENTITY AND PRIVILEGE MANAGEMENT** (GFIPM), referenced throughout this document, and privacy and civil liberties protections. These documents, while associated with various components of the GRA, work in concert

and have been rationalized to ensure mutual support of the information sharing enterprise and consistent guidance across the range of resources.

Value to the Justice Community: By providing a robust roadmap to an understanding of what should be considered for inclusion in each section of the SLA, including an example of expectations and obligations for those offering or using a fingerprint service within the GJISE, it is hoped practitioners will receive the full benefits of "reuse"—drastically reduced time devoted to research and development of their own SLAs, even if the service being considered is not a fingerprint service (see *Additional Notes and Caveats,* following). Of course, this document is an example, and it can be tailored to best meet an organization's specific governance needs.

Additional Notes and Caveats: It is anticipated that individual SLAs will be created for categories of similar services as opposed to each discrete service. It is also anticipated that these categories will be based on fundamental characteristics the services have in common, such as *public* versus *nonpublic* data and service response criteria such as *real-time* and *less than real-time* service. Further recommendations on service categories are forthcoming.

As previously noted, this example addresses a fingerprint service SLA, where one party is clearly the service **PROVIDER**, and one party is the service **CONSUMER**. However, this delineation is not always so clear-cut, particularly when *data stewardship* is part of the service. When this additional consideration is added, a service provider can then be a primary data provider, data consumer, or both. Likewise, a service consumer can be a primary data consumer, data provider, or both. Additionally, a primary consumer can also be a secondary provider—or redistributor—to other tertiary parties (a role associated with "travelling data policies" and associated obligations). While this issue will not be explored or addressed in more detail in this document, the authors want to ensure due diligence by noting this fact in the event that a practitioner uses this SLA and encounters the same deviation from straight "provider" and "consumer" categorization. The sections of this SLA most likely to be affected by this issue are ***3. Service Availability, Response Time, and Throughput***; ***6. Eligibility, Access, Acceptable Use, and Security***; ***8. System of Record, Confidentiality, Audit, and Expungement***; and ***9. Data Quality***.

A next step for the GISWG M&P Committee, in addition to release of the SLA template, will be development of an alternate SLA example, more fully exploring issues associated with the secondary provider/redistributor role and proffering another example for practitioners entering into an SLA under those circumstances.

1. Purpose

This **SERVICE-LEVEL AGREEMENT** (SLA) governs the specific terms and conditions around the provision and consumption of a **FINGERPRINT SERVICE** within the **GLOBAL JUSTICE INFORMATION SHARING ENTERPRISE** (GJISE) and extends the governing **GJISE STATEMENT OF PARTICIPATION** (Statement of Participation). It identifies the rights and obligations of the fingerprint service provider *["insert service provider name"]* (**PROVIDER**) and service user *[insert service user name]* (**CONSUMER**). By reference, **PROVIDER** and **CONSUMER** agree to be bound by the Statement of Participation and related agreements; warrant that the Statement of Participation has the authority to so bind; and have the capacity to comply with the Statement of Participation.

In the context of the **GLOBAL REFERENCE ARCHITECTURE** (GRA) and a service-oriented architecture in general, a SERVICE is the means by which one partner gains access to one or more business-related specific **CAPABILITIES** offered by another partner. Service capabilities create or generate a **REAL-WORLD EFFECT** that can be as simple as sharing information or involve performing a function or changing the condition of some other processes. In the context of this SLA, the Fingerprint Service provides positive identification or verification of a person's identity based on the submission of fingerprint information. The service receives one or more fingerprint images and returns a biometrically based response, facilitating the determination of the physical identity of an individual. Therefore, the capabilities are:

- Provides biometrically based identification.
- Provides biometrically based verification.

Examples of real-world effects are:

1. Law enforcement agencies can use this service as part of the criminal apprehension arrest process.
2. Courts can use this service during the court appearance and bond hearing processes.

The term of this agreement is effective *["insert date that the agreement is binding"]*. Changes, as necessary, will be made through subsequent agreements or amendments to this document.

2. Fingerprint Service Version and Documentation

The Fingerprint Service referenced in this SLA is defined by the **FINGERPRINT (FP) SERVICE V 0.9.3 SERVICE DESCRIPTION DOCUMENT** or current version.[1] The service interface description is governed by **FINGERPRINT (FP) SERVICE V.0.9.3 SERVICE INTERFACE DESCRIPTION DOCUMENT**, or current version.[2]

[1] Please see http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015, **Reference Service Specification Packages (SSPs), Fingerprint (FP) Service Specification** section for the most current version.
[2] *Ibid.*

3. Service Availability, Response Time, and Throughput

3.1. PROVIDER Obligations

3.1.1. Service Availability

PROVIDER shall ensure service availability as follows:

An outage of this service would have critical impact on public safety, would be highly visible, and would affect a significant number of users, agencies, services, or applications. As such:

- This service is offered 24 hours a day, 7 days a week, 365 days per year (24x7x365).
- This service does not have a maintenance window.
- Notification will typically be given at least 48 hours before planned maintenance.

3.1.2. Service Support

PROVIDER shall ensure service support as follows:

- First-level service support is available from the Livescan vendor 24x7.
- If the Livescan vendor is unable to resolve the issue, contact the Service Desk (24x7) at the number listed in subsection ***4.2.1. Problem Reporting*** of this document.

3.1.3. Response Time and Throughput

PROVIDER will ensure service performance level as follows:

- **Livescan:** 90 percent of submissions will not exceed 10 minutes to return identification information with remaining submissions complete within an average of one hour. This response time is limited by the volume capacity described in section ***3. Service Availability, Response Time, and Throughput*** of this document and excludes technical issues covered in section ***4. Problem Reporting and Resolution; Escalation Procedures.***

- **Paper:** 100 percent of submissions will not exceed five business days from receipt at the agency to return identification information.

- **Throughput/System Volume Capacity:** **PROVIDER** agrees to support 1,800 submissions per day, 360 maximum per hour (all users combined). Beyond this capacity, all users may see degraded performance in the return of identification information.

3.2. CONSUMER Obligations

3.2.1. Connectivity

CONSUMER agrees to maintain connectivity as follows:

- Livescan devices are physically connected to the submitting agency infrastructure. Submitting (i.e., CONSUMING) agencies are expected to maintain connectivity between the Livescan and the State Data Network.

- The **CONSUMER** will acquire and maintain a network (Internet/Private) interface to *["insert network name"]*, will utilize one of the access mechanisms defined in section ***6. Eligibility, Access, Acceptable Use, and Security*** of this document, and will comply with the **GRA RELIABLE SECURE WEB SERVICES SERVICE INTERACTION PROFILE.**[3]

- The **CONSUMER** will financially sustain and maintain all equipment and network services during the life of this agreement.

3.2.2. Information Technology (IT) Support

CONSUMER agrees to maintain IT support as follows:

- The submitting agency is expected to assign technical staff in a timely manner to assist **PROVIDER** agency or vendor staff in

[3] Please see www.it.ojp.gov/GRA_Reliable_Secure_Web_Services_SIP. The purpose of this document is to establish a reliable secure Web services **SERVICE INTERACTION PROFILE (SIP)** based on the Web services family of technology standards and, in particular, the Web Services Interoperability Organization Reliable Secure Profile (WS-I RSP).

troubleshooting technical problems with either the Livescan or connectivity.

4. Problem Reporting and Resolution; Escalation Procedure

4.1. PROVIDER Obligations

4.1.1. Resolution

An acknowledgement will be sent by the help desk within 30 minutes of receipt of the problem report. Problems will be categorized as **CRITICAL PROBLEMS** and **NONCRITICAL PROBLEMS** with corresponding resolution parameters.

- **CRITICAL PROBLEMS** are defined as disruptions of service where the **CONSUMER** no longer has access to the service.

- **NONCRITICAL PROBLEMS** are all other problems that impede or degrade service delivery but do not result in a service disruption.

PROVIDER will resolve problems as follows:

- Critical problems occurring during work hours: If not resolved within 120 minutes, the problem will escalate to reporting to **PROVIDER** management identified in section ***16. Notices*** of this document for resolution.

- Critical problems occurring after hours: If not resolved within 240 minutes, the problem will escalate to reporting to **PROVIDER** management identified in section ***16. Notices*** of this document for resolution.

- Noncritical problems: If not resolved within two workdays, the problem will escalate to reporting to **PROVIDER** management identified in section ***16. Notices*** of this document for resolution.

  In the event the **CONSUMER** has escalated nonresolution of a problem to **PROVIDER** management (identified in section ***16. Notices*** of this document) per the procedure outlined in the following subsection, the **PROVIDER** will respond within one business day with an assessment of the problem and an estimated resolution time.

4.2. CONSUMER Obligations

4.2.1. Problem Reporting

In the event a problem or disruption (as defined in the preceding subsection) or another issue occurs, the **CONSUMER** shall:

- Report the problem to the Service Provider Help Desk at the contact points below:
  - Telephone: ["*insert complete phone number, including area code, of Service Provider Help Desk*"] or toll free: [*if available; "insert complete phone number, including toll-free area code, Service Provider Help Desk"*]
  - E-mail: ["*insert e-mail address of Service Provider Help Desk*"]

4.2.2. Escalation Procedure

If a problem is not resolved within the time limits for critical and noncritical problems as defined in the preceding subsection, the **CONSUMER** may:

- Contact **Help Desk Management** to escalate the resolution of the problem. This may be reported at the contact points below:
  - Telephone: ["*insert complete phone number, including area code, of Help Desk Management*"] or toll free: [*if available; "insert complete phone number, including toll-free area code, of Help Desk Management"*]
  - E-mail: ["*insert e-mail address of Help Desk Management*"]

5. Change Control

5.1. PROVIDER Obligations

5.1.1. Changes and Notice

- The **PROVIDER** shall exert the best effort to provide 60 days notice to **CONSUMERS** who have registered with the **PROVIDER** prior to making any changes.

- Changes may occur without notice to **CONSUMERS** who are not registered with the **PROVIDER.**

5.1.2. Versioning

PROVIDER shall:

- Maintain each version of the service specification in the **PROVIDER** repository and shall ensure that the prior four versions of the service specification are available in the repository and are operational.

- Maintain an active version of a service for at least 24 months from release date.

5.1.3. Documentation

PROVIDER shall:

- Document, maintain, and publish its change control process.

5.2. CONSUMER Obligations

5.2.1. Version Currency

CONSUMER will make the best effort to:

- Utilize the most recent release within six months of general availability. **CONSUMERS** using versions not maintained by the **PROVIDER** are subject to loss of access to the service.

6. Eligibility, Access, Acceptable Use, and Security

6.1. Overall Obligations

PROVIDER and **CONSUMERS** agree to adhere to the **GLOBAL FEDERATED IDENTITY AND PRIVILEGE MANAGEMENT** (GFIPM) principles and protocols.

It is both a **PROVIDER'S** and a **CONSUMER'S** obligation to maintain acceptable use.

Overall Obligations
The Fingerprint Service utilizes role-based access and privilege control. Therefore, it is expected that an SLA for this type of service will utilize GFIPM.

General Conformance to GFIPM Policies
The objective of the **GFIPM** standards and specifications is to provide a security framework for securely connecting justice and public safety personnel to interagency applications and data over the Internet. Federation is a fundamental concept within the GFIPM framework.

Two GFIPM documents addressing governance and management issues have intersections with this SLA:

- The **U.S. Department of Justice's Global Federated Identity and Privilege Management Governance Guidelines (GFIPM GOV),** which identifies the different parties involved in the **GOVERNANCE** of a federation, and defines the necessary decisions by these parties.
- The **U.S. Department of Justice's Global Federated Identity and Privilege Management Operational Policies and Procedures (GFIPM OPP)**, which describes the operational policies and procedures that govern the basic operation of a federation for trusted identity and authentication attributes for information sharing. Specifically, the policies and procedures in this document are focused on creating and maintaining a solid foundation of trust on which an information sharing infrastructure can be built and operated.

Both are available at http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1179.

6.2. PROVIDER Obligations

6.2.1. General—Conformance to GFIPM Policies

The **PROVIDER** agrees to provision its services in accordance with the **GLOBAL FEDERATED IDENTITY AND PRIVILEGE MANAGEMENT OPERATIONAL POLICIES AND PROCEDURES GUIDELINES** (GFIPM OPP). These services will be accessible to **IDENTITY PROVIDER** (IDP) end users who meet the requirements of an established and documented access policy that the **PROVIDER** has defined. Unless the **PROVIDER** has specifically identified certain or all of its services that are not public,[4] the **CONSUMER** may publicize the services which the **PROVIDER** has made available. However, **PROVIDERS** who need to keep the availability of their service(s) confidential may specify the set of required attributes for discovery of their services in any applicable directory of services. At all times that the **PROVIDER** is a party to this agreement, it agrees to abide by the GFIPM OPP. Specifically, the **PROVIDER** agrees to meet minimum security and availability standards. The **PROVIDER** agrees to comply with any decisions made through the governance process, in accordance

[4] The **FINGERPRINT SERVICE** governed by this SLA is not public.

with the **GLOBAL FEDERATED IDENTITY AND PRIVILEGE MANAGEMENT GOVERNANCE GUIDELINES** (GFIPM GOV).

6.2.2. Access/Acceptable Use

PROVIDERS shall:

- Have the capability to validate identity assertions that are submitted by **IDENTITY PROVIDERS** (IDP) as part of a service request.
- Have the ability to define attributes that IDPs must present for access to the service.
- Have the capability to react to receipt of various requestor assertions based on the established policy.

All **PROVIDERS** must certify that they are providing only information or services that they have legal rights to provide.

See Overall Obligations, particularly with reference to the **GLOBAL FEDERATED IDENTITY AND PRIVILEGE MANAGEMENT GOVERNANCE GUIDELINES** (GFIPM GOV) minimum security requirements.

6.3. CONSUMER Obligations

6.3.1. General

CONSUMERS must:

- Possess a valid Originating Identification Number (ORI).
- Acquire and support the equipment needed to participate in this service (i.e., National Institute of Standards and Technology [NIST]-conformant fingerprint capture device[s]).
- Put in place documented procedures for screening, restricting, inspecting, and enforcing the proper use of this service, and shall establish access control criteria to ensure that their personnel who are authorized to access this service remain compliant in their access to and use and management of service data. These criteria shall be personnel-centric and include proper usage of passwords, functional-level access, and restriction on noncompliant devices.

- Establish agencywide access control mechanisms to ensure that the **CONSUMER'S** agency maintains proper records of both personnel and computers that are interfacing with this service. These criteria shall be agency-centric and include controls for updated lists of all personnel authorized to access this service, as well as measures for strict cryptographic key management so that only those personnel with authorization to decrypt encrypted data can do so.

6.3.2. Privileges/Acceptable Use

CONSUMER can lawfully utilize one or more of the following **PRIVILEGES**[5]:

- Counter Terrorism Data Privilege
- Criminal History Data Privilege
- Criminal Investigation History Data Privilege
- Criminal Intelligence Data Privilege
- Justice Data Privilege

Privileges/Acceptable Use
The Fingerprint Service is a criminal justice-only service, not identification for licensing or employment purposes. Therefore, this SLA includes reference to a privilege policy component. GFIPM is the method to enforce this obligation.

This subsection would not be included for noncriminal justice services.

6.3.3. Security

CONSUMER shall conform to the following security policies:

- **GLOBAL FEDERATED IDENTITY AND PRIVILEGE MANAGEMENT GOVERNANCE GUIDELINES** (GFIPM GOV)
- **FEDERAL BUREAU OF INVESTIGATION (FBI) CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SECURITY POLICY**[6]
- [*insert appropriate State(s) Bureau of Criminal Identification Privacy and Security Policies*]

[5] The list of privileges is based on purpose codes contained in the National Crime Information Center (NCIC) 2000 Interstate Identification Index (III), Section 2.1. NCIC code lists and indices are available to local, state, and federal law enforcement and other criminal justice agencies. See http://www.fbi.gov/hq/cjisd/ncic.htm for more on NCIC.

[6] The FBI CJIS Security Policy is considered to be sensitive but unclassified (SBU) material. This policy may not be posted to a public Web site, and discretion must be exercised in sharing the contents of the policy with individuals and entities who are not engaged in law enforcement or the administration of criminal justice.

7. Governance and Authority

Overall governance and authority over this service is the responsibility of the [*insert governing program's title*] Program and is defined in the [*insert governing program's title*] Program GJISE Statement of Participation. Specific service obligations within this overall governance are defined herein.

8. System of Record, Confidentiality, Audit, and Expungement

8.1. Overall Obligations

PROVIDER and **CONSUMER** agree to adhere to the Global privacy principles and protocols, such as those contained in the **GLOBAL PRIVACY AND CIVIL LIBERTIES POLICY DEVELOPMENT GUIDE AND IMPLEMENTATION TEMPLATES.**

Overall Obligations
The **Global Privacy and Information Quality Working Group** (GPIQWG) has developed many policies, guidelines, and templates to assist agencies in meeting the appropriate privacy best practices and comply with federal and state privacy laws. The GPIQWG's body of work should be consulted when providing and consuming services and is available at http://it.ojp.gov/default.aspx?area=privacy.

Provider Obligations
Preserving appropriate privacy and acceptable use is critical to justice information sharing. The PROVIDER maintains the system of record, is the owner of the data, and receives Freedom of Information Act (FOIA)-associated requests. Global privacy best practices assign these obligations to the data provider.

8.2. PROVIDER Obligations

8.2.1. System of Record and Confidentiality

The **PROVIDER** maintains the System of Record for this service and is the owner of the data. The **PROVIDER** shall adhere to the confidentiality and use limitation (see section ***6. Eligibility, Access, Acceptable Use, and Security***) for the **PERSONALLY IDENTIFIABLE INFORMATION** (PII) as maintained in the **SYSTEM OF RECORD NOTICE** (SORN), or the data practices laws of the agency for this system of record.

8.3. CONSUMER Obligations

8.3.1. Confidentiality

The **CONSUMER** shall preserve the confidentiality of and limit access to data consumed from this service in accordance with the **PROVIDER SORN**, or data practices laws of the agency of the system of record; a traveling data policy or secondary dissemination policy, if any; or the data practices laws of the consumer system.

8.3.2. Audit

CONSUMERS of the Fingerprint Service must maintain an audit trail containing, at a minimum, the following:

- The GFIPM User Assertion-User Federation Profile, or equivalent[7]
- Privilege category (see section ***6. Eligibility, Access, Acceptable Use, and Security***), FBI National Crime Information Center Purpose Code, or equivalent
- Date and time of transaction
- Transaction number
- All request transaction data and all response record data

The **CONSUMER** shall maintain this data for a period of five years. This data must be made accessible in **NATIONAL INFORMATION EXCHANGE MODEL** (NIEM) 2.0 or later version within 72 hours of a request from the authorized agent of the **PROVIDER**.

To update or modify any previously provided information, the **CONSUMER** agency shall perform an ongoing validation of the returned information.

8.3.3. Expungement

The **CONSUMER** will comply with expungement orders as follows:

- The submitting (i.e., **CONSUMER**) agency shall notify the **PROVIDER** of any received seal or expungement orders within two working days of receipt and will certify to **PROVIDER** the execution of the order immediately upon compliance.

8.3.4. Freedom of Information Act (FOIA) Requests

The **CONSUMER** will comply with FOIA requests as follows:

[7] See **Global Federated Identity and Privilege Management (GFIPM) Metadata Specification Version 1.0**, located at http://it.ojp.gov/documents/GFIPM-Metadata-1.0.zip.

- The **CONSUMER** will direct the requesting party back to the **PROVIDER**.

9. Data Quality

9.1. PROVIDER Obligations

9.1.1. FALSE RETURNS

The **PROVIDER** will:

- Return criminal identification and rap-sheet data. Identification will be less than 0.1 percent false positives and 0.2 percent false negatives. Rap-sheet data will be of no lesser quality than that submitted to the service or direct submission to the **PROVIDER**. The **PROVIDER** reserves the right to reject submissions because of data-quality issues.

- Reject and return to the **CONSUMER** all prints that do not meet **PROVIDER**-published standards in addition to the National Institute of Standards and Technology (NIST) standard.

9.2. CONSUMER Obligations

9.2.1. Fingerprint Capture NIST Standard

The **CONSUMER** will:

Make submissions in accordance with the Fingerprint Service, as described in the Global Reference Architecture (GRA) Fingerprint (FP) Service Description Document v 0.9.3 or current version, which incorporates the NIST biometric standards.

Fingerprint Capture NIST Standard

The FINGERPRINT SERVICE leverages the Electronic Biometric Transmission Specification (EBTS) NIEM Information Exchange Package Documentation (IEPD) created by the FBI CJIS Division.

- The EBTS is the method by which the FBI supports the exchange of biometric data used to facilitate the determination of the personal identity of a subject from fingerprint, palm, facial, or other biometric information, across criminal justice agencies or organizations that use an Automated Fingerprint Identification System (AFIS) or related systems nationwide. These biometric specifications are standards for electronically encoding and transmitting biometric image, identification, and arrest data.
- The FBI EBTS comprises the biometric standards titled *Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information (ANSI/NIST-ITL 1-2007)*, which are composed by the American National Standards Institute (ANSI) in correspondence with the Information Technology Laboratory (ITL) of NIST.

9.2.2. Demographic, Charge, and Disposition Data

The **CONSUMER** will:

- Make best efforts to submit accurate biometric and demographic information, as appropriate, to enable positive identification or verification of the physical identity of an individual.
- Depending on the nature of the action, independently verify data that is returned by the **PROVIDER**.

9.2.3. Livescan Table Updates

For G3 Livescans, the **CONSUMER** will:

Update information on Livescans via the agency's Livescan Centralized Management (LCM) Service to maintain the most current information available. These updates include tables such as ORI lists, NCIC code lists, and statutes. LCM is also capable of updating the Livescan software. For table updates, the normal operation of the Livescan should not be interrupted. For software updates, the operator may be required to either exit the Livescan application and restart or reboot the Livescan.

Definition
The service governance authority (in this case, the GJISE) and the companion Statement of Participation for this criminal justice service is founded on the standards and corrective actions recommended by the FBI and NCIC to ensure compliance with this service-level agreement. This example SLA attempts to incorporate these recommendations.

9.2.4. Identification Challenges

If a **CONSUMER** has information that leads him or her to question a **PROVIDER**-determined identification, the **CONSUMER** should:

- Contact the **PROVIDER**. The **PROVIDER** will review the fingerprints used in making the identification and communicate the results to the **CONSUMER**.

9.2.5. Court Testimony

If the **CONSUMER** receives a court challenge to fingerprint-based identification(s) made via this service, the **PROVIDER** will:

- Testify in court as to the accuracy of the identification.

- To that end, the **CONSUMER** must contact the **PROVIDER** at least five business days prior to the court date and provide the Livescan Booking Identification Number (Booking ID or BID), date of the booking, subject's name and date of birth, and other necessary information.

10. Nonconformance and Rights Upon Assertion or Determination of Nonconformance

10.1. Definition

NONCONFORMANCE is defined as a failure to abide by or adhere to all obligations of the service governed herein: violations of law of either the **PROVIDER** or the **CONSUMER** and other violations as defined in this section include:

10.1.1. Acts of Consumer Nonconformance

- Failure to abide by Access Control and Security Policies.
- Failure to respond to corrective actions within the allotted time as defined in this SLA and other governing documents.
- Failure to respond to audit findings within the allotted time as defined in this SLA and other governing documents.
- Failure to perform proper security clearance practices for agency personnel.
- Failure to properly monitor use of the service.

10.1.2. Acts of PROVIDER Nonconformance

- Repeated failure to respond to and remedy reported problems and errors.

10.2. PROVIDER Rights Upon Assertion or Determination of CONSUMER Noncompliance

The **PROVIDER** may:

- Send a letter to the **CONSUMER,** as identified in section ***16. Notices*****,** documenting the infractions and corrective actions required.

- Provide Notice of Provisional Status after repeated failure to resolve corrective actions.

- Provide Notice of Intent to Terminate Service Participation.

- Terminate Service Participation with either the **CONSUMER** agency, as a whole, or individual employees of the agency.

- Terminate Service Participation without prior notification in the event of a **SERIOUS BREACH** (i.e., nonresponse to the notices outlined, above) of this agreement.

10.3. CONSUMER Rights Upon Assertion or Determination of PROVIDER Noncompliance

The **CONSUMER** may:

- Request and receive reports documenting performance metrics as defined in section ***3. Service Availability, Response Time, and Throughput***

- Escalate problems per section ***4. Problem Reporting and Resolution; Escalation Procedure***

- Terminate participation and:
  - Recover all costs for any unused portion of the outstanding term of service.

  - Receive any equipment owned by the **CONSUMER** from within the shared execution context of this service.

There are no other corrective actions expressed or implied within the scope of this Service Level Agreement.

11. Durability of Service

The **PROVIDER** recognizes that the services provided under this SLA are very important to the **CONSUMER** and that the goal and intent of the parties is to continue

such services without interruption and that, upon SLA expiration, a successor—whether a governmental agency or another private entity—may continue those services.

11.1. Definition of Transition Period

Prior to the end of the SLA term, and in the event that the **PROVIDER** under this agreement plans to discontinue provision of services to the **CONSUMER**, there will be a Transition Period with the following obligations.

11.2. PROVIDER Obligations

During the Transition Period, the **PROVIDER** will:

- Make an orderly transition of the service, and perform any and all tasks in good faith that are necessary to preserve the integrity of ongoing **CONSUMER** operations.
- Make every reasonable effort to ensure that any such transition shall be performed in a professional and businesslike manner.
- Comply with the reasonable requests and requirements of the **CONSUMER**, and any successor **PROVIDER**, with the intent and goal of accomplishing a successful, seamless, and unhindered transfer of responsibilities.

11.3. CONSUMER Obligations

During the Transition Period, the **CONSUMER** will:

- Make continued payment of the ordinary and usual compensation for the continued use of the Service.
- Comply with any other Consumer Obligations, as specified herein.

12. Fees and Costs

12.1. PROVIDER Obligations

12.1.1. Rate Schedule

Fees for the use of the services provided in this SLA will use the rates incorporated in the **PROVIDER'S** approved rate schedule attached as **Attachment A-1** [*insert rate*

schedule as attachment] to this SLA. The fee schedules included in **Attachment A-1** are inclusive of:

- One-time or connection fees
- Periodic fees
- Transaction fees
- Service context fees
- Deposits
- Payments
- Late fees and interest fees
- Accounting fees and payments
- Periodic billing and invoicing
- Credits and refunds
- Equipment fees incurred
- Professional service fees

12.1.2. Fee Changes

Fees are subject to change with a 60-day notice from the **PROVIDER** to the **CONSUMER**.

12.2. Customization of Services and Fees

Customization of services to meet the written requirements of the **CONSUMER** may be provided by the **PROVIDER** and are subject to project management fees (which will be agreed to by the parties) and development fees, per the rate schedule attached as **Attachment A-1**, on a time and materials basis.

12.3. Additional Considerations

Revisions, ongoing maintenance, and performance standards shall be addressed in additional agreements that are incorporated by reference in this SLA.

13. Liability

The **PROVIDER** shall not be liable to the **CONSUMER** for any direct, indirect, incidental, special, consequential, or exemplary damages, including, but not limited to, damages for loss of life, profits, goodwill, use, data, or other losses (even if the **PROVIDER** has knowledge of the possibility of such damages) in connection with this service, including, without limitation, any such damages resulting from:

- Use or inability to use the service.

- Cost of procurement of substitute services.
- Unauthorized access to or alteration of the **CONSUMER** content.

In any case, the aggregate liability under this agreement shall be limited to the amount actually paid by the **CONSUMER** to the **PROVIDER.**

14. Governing Law, Jurisdictions, and Disputes

This SLA shall be construed in accordance with and governed by the laws of the [*insert PROVIDER's state*].

14.1. General

14.2. Dispute Resolution

It is the intent of the parties that any disputes that may arise between them beyond those to be resolved by, or unable to be resolved by, section ***4. Problem Reporting and Resolution; Escalation Procedure*** or section ***10. Nonconformance and Rights Upon Assertion or Determination of Nonconformance*** be resolved as quickly as possible. Quick resolution may, in certain circumstances, involve immediate decisions made by the parties' duly authorized representatives. When such resolution is not possible and depending upon the nature of the dispute, the parties hereto agree to resolve such disputes in accordance with the following provisions:

- Any **Disputed Issues** concerning this SLA shall in all instances be initially referred to the parties' designated representatives identified in the SLA. The parties' designated representatives shall use reasonable best efforts to render a mutually agreeable resolution of the disputed issue, in writing, within three business days of such referral.

- **PROVIDER Obligation** is to continue to perform pursuant to this SLA during any dispute resolution proceedings, subject to the provisions of this Contract.

- **Unresolved Disputes** will be submitted to the GJISE for arbitrated resolution and if not resolved by GJISE, will be resolved according to law as specified above.

15. Order of Precedence

Terms and conditions that apply must be in writing and attached to the SLA. No other terms and conditions will apply to this SLA including terms listed or referenced on memoranda of understanding or other similar agreements. In the event of any conflict in the SLA terms and conditions, the order of precedence shall be:

- First, this SLA and any referenced attachments; then,
- Terms and conditions of the **PROVIDER**; then,
- Terms and conditions of the **CONSUMER**; and
- Any other related Service Contracts associated with the **PROVIDER** or **CONSUMER.**

16. Notices

The following named party is designated to receive notices on behalf of the **PROVIDER**:

[insert individual name]
[insert organization name]
[insert mailing address]
[insert phone number]
[insert e-mail address]

The following named party is designated to receive notices on behalf of the **CONSUMER**:

[insert individual name]
[insert organization name]
[insert mailing address]
[insert phone number]
[insert e-mail address]

Each party may change its designation for notice by written notice to the other parties.

Notices by the parties to one another shall be given in writing to the persons identified above or to such other persons as may be subsequently identified in a written notice. Such notices shall be effective on the date of mailing or transmission

if sent by U.S. first-class or restricted delivery mail; postpaid, certified mail, return receipt requested; or by any reputable overnight delivery service, prepaid, or by facsimile transmission or electronic mail if proof of transmission is retained.

Notices pertaining to legal matters including, but not necessarily limited to, termination, default, or liability shall be sent in compliance with applicable law, if different than the provisions of this SLA, and via prepaid, certified mail, return receipt requested.

17. Signature Section/Contract Authority

IN WITNESS WHEREOF, the parties having read and understood the foregoing sections of the SLA including all documents and exhibits incorporated therein by reference, expressly agree to these terms and conditions as evidenced by their respective dated signatures below:

PROVIDER

_____

Signature

_____

Printed Name

_____

Title

_____

Date

CONSUMER

_____

Signature

_____

Printed Name

_____

Title

Date

[*"Insert witness and/or notary language and/or signature, if necessary, to validate the above signatures."*]

18. Resources and Definitions

False Returns—In a Fingerprint Service query, false returns are returns in which an individual is incorrectly deemed *to have* a record (false positive) or in which an individual is incorrectly deemed *to not have* a record (false negative).

Fingerprint Service—The Fingerprint Service provides positive identification or verification based on the submission of fingerprint information. The service receives one or more fingerprint images and returns a biometrically based response, which facilitates the determination of the physical identity of an individual.

- **Identification** is defined as the capability to compare a biometric object against a biometric information repository for a biometric match to determine biometric-based identity (as compared with name and date of birth identity, for example).

- **Verification** is defined as the capability to compare a biometric object and a biometrically based identifier against a biometric information repository for a biometric match to verify assertions of identity.

In many cases, in addition to the biometric object and the biometrically based identifier, additional information is submitted to the service to allow for search optimization. This information could be personal demographic information or geographic location information.

See www.it.ojp.gov/Fingerprint_Service_Specification.

Global Federated Identity and Privilege Management (GFIPM)—The Global Federated Identity and Privilege Management (GFIPM) framework provides the justice community and partner organizations with a standards-based approach for implementing federated identity. The concept of globally understood metadata across federation systems is essential to GFIPM interoperability. Just as a common Extensible Markup Language (XML) data model was the key to data interoperability, a standard set of XML elements and attributes about a federation user's identities,

privileges, and authentication can be universally communicated. The GFIPM metadata and framework support the following three major interoperability areas of security in the federation:

- Identification/Authentication—*Who is the end user and how was he or she authenticated?*
- Privilege Management—*What certifications, clearances, job functions, local privileges, and organizational affiliations are associated with the end user that can serve as the basis for authorization decisions?*
- Audit—*What information is needed or required for the purposes of auditing systems, systems access and use, and legal compliance of data practices?*

See http://it.ojp.gov/GFIPM for more on GFIPM.

Global Federated Identity and Privilege Management Governance Guidelines (GFIPM GOV)—This document identifies the different parties involved in the governance of a federation and defines what decisions will be made by these parties. The parties involved in the governance are the board of directors, federation management, service providers, and identity providers**.**

See www.it.ojp.gov/GFIPM_Governance_Guidelines.

Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines (GFIPM OPP)—This document describes the operational policies and procedures that govern the basic operation of a federation for trusted identity and authentication attributes information sharing. Specifically, the policies and procedures in this document are focused on creating and maintaining a solid foundation of trust on which an information sharing infrastructure can be built and operated. The target audience for this document includes representatives of prospective federation participants who intend to join the federation as identity providers (IDPs), service providers (SPs), or both, as well as current members.

See www.it.ojp.gov/GFIPM_Operational_Policies_and_Procedures.

Global Justice Information Sharing Enterprise (GJISE)—Any group of business entities that pursue common business objectives through the sharing of information. This could be a county or city justice information sharing initiative, a statewide initiative, a tribal (or multitribe) initiative, a regional initiative, or a national initiative.

GJISE Statement of Participation—This document provides a reference model framework of expectations and obligations for those entities participating in any state, local, regional, or tribal information sharing enterprise. An information sharing enterprise is a consortium of information service providers and service consumers created specifically to engage in trusted and secure information sharing across disparate justice systems. With minimal modification, this document can be adopted by any information sharing enterprise offering or using information services.

See www.it.ojp.gov/GJISE_Statement_of_Participation.

Global Privacy and Civil Liberties Policy Development Guide and Implementation Templates—Geared toward practitioners charged with developing or revising their agency's privacy policy, this document is a practical, hands-on resource and is the next logical step for those justice entities that are ready to move beyond awareness into the actual policy development process. It assists agencies in articulating privacy obligations in a manner that protects the justice agency, the individual, and the public and makes it easier to do what is necessary–share critical justice information. The Implementation Templates included in this document are an essential tool for justice system practitioners to use during the drafting process.

See http://it.ojp.gov/documents/Privacy_Guide_Final.pdf.

Identity Provider (IDP)—An entity that vets individuals, collects attributes about these individuals, and maintains these attributes in an accurate and timely manner. The IDP performs user authentication each time an individual presents himself to the federation and assigns the current attributes about the individual for a given information technology session. These attributes are presented to Service Providers in the federation or on a federation-to-federation basis.

Global Reference Architecture—The Global Reference Architecture (GRA) is an abstract framework for understanding significant components and relationships between them within a service-oriented environment. It lays out common concepts and definitions as the foundation for development of consistent service-oriented architecture (SOA) implementations within the justice and public safety communities.

See www.it.ojp.gov/GRA_Spec_1-7.

National Information Exchange Model (NIEM)—The National Information Exchange Model (NIEM) is a local, state, tribal, and federal interagency initiative providing a foundation for seamless information exchange, and was launched on February 28, 2005, through a partnership agreement between the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS) and signed

by Chief Information Officers. It leverages the data exchange standards efforts successfully implemented by the Global Justice Information Sharing Initiative (Global) and extends the Global Justice XML Data Model (GJXDM) to facilitate timely, secure information sharing across the whole of the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise. See http://www.niem.gov.

Personally Identifiable Information (PII)—PII is information that can be used to uniquely identify, contact, or locate a single person or that can be used with other sources to uniquely identify a single individual.

Service Consumer (CONSUMER)—An entity in the GJISE that consumes a service provided by the provider entity.

Service Interaction Profile (SIP)—A SIP is a concept identified in the Global GRA, defining an approach to meeting the basic requirements necessary for interaction between **CONSUMERS** and **SERVICES**. The approach utilizes a cohesive or natural grouping of technologies, standards, or techniques in meeting those basic interaction requirements. A profile establishes a basis for interoperability between service consumer systems and services that agree to utilize that profile for interaction. A SIP guides the definition of **SERVICE INTERFACES**. In a service-oriented architecture (SOA) environment, every service interface shared between two or more information systems should conform to exactly one service interaction profile. **CONSUMERS** that interact with an interface should likewise conform to that interface's profile.

Service Provider (PROVIDER)—An entity in the GJISE that provides a consumable service to a consumer entity.

System of Record Notice (SORN)—A System of Records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. The Privacy Act requires each agency to publish notice of its systems of records in the Federal Register. This notice is generally referred to as a system of records notice (SORN).

Attachment A-1

[*insert rate schedule as attachment*]

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

For more information on DOJ's Global and its products, including those referenced in this document, call

(850) 385-0600

or visit

www.it.ojp.gov/globaljra

BJA

Bureau of Justice Assistance
U.S. Department of Justice