FRONT COVER—

Federated Identity and Privilege Management, Governance Guidelines, Version 1.1, April 2012

Global Information Sharing Standard

**DEPRECATION NOTICE**

This document has been deprecated by the GFIPM Task Team (see <https://it.ojp.gov/initiatives/gfipm>). The GFIPM Task Team no longer recommends the organization of new GFIPM federations within the justice community, as this approach tends to fracture the community by creating unnecessary federation boundaries between would-be information sharing partners that belong to different federations. In lieu of establishing a new federation, the GFIPM Task Team now recommends that agencies adopt a componentized, decentralized approach to federated trust, similar to the trustmark-based approach that the National Identity Exchange Federation (NIEF) (see <https://nief.org/>) has adopted. For more information and guidance about how to pursue this approach, please contact [help@gfipm.net](mailto:help@gfipm.net).

INSIDE COVER—

Global Standards

Global’s collection of normative standards has been versioned independently and assembled into a package of composable, interoperable solutions specifically supporting an information exchange.  The package is known as the Global Standards Package (GSP).  GSP solutions are generally technically focused but also may include associated guidelines and operating documents.  GSP deliverables include artifacts associated with many of the Global product areas, including but not limited to:
•  Global Reference Architecture (GRA):  Offers guidance on the design, specification, and implementation of services (and related infrastructure) as part of a justice Service-Oriented Architecture (SOA). 
•  Global Service Specification Packages (SSPs):  Reference services that serve as the means by which the information needs of a consumer are connected with the information capabilities of an information provider.
•  Global Federated Identity and Privilege Management (GFIPM):  Guidelines and standards for establishing, implementing, and governing federated identity management approaches. 
•  Global Privacy Technology Framework:  A framework for automating access control (in particular, privacy) policy as part of information exchange.

For More Information
For more information on the GSP and the Global Standards Council (GSC)—the Global group responsible for developing, maintaining, and sustaining the same—please visit http://www.it.ojp.gov/gsc. 


About the Document

Justice organizations are looking for ways to provide secured access to multiple agency information systems with a single logon. The Global Federated Identity and Privilege Management (GFIPM) initiative, developed by the U.S. Department of Justice’s Global Justice Information Sharing Initiative, provides the justice community with a security and information sharing architecture that is based on an electronic justice credential. This standards-based justice credential can be used to securely connect law enforcement and public safety personnel to interagency applications and data over the Internet.

**Background:** The GFIPM framework provides the justice community and partner organizations with a standards-based approach for implementing federated identity. Common use of these standards across federation systems is essential to their interoperability. Leveraging the Global Justice XML and National Information Exchange Model (NIEM), a standard set of XML-based elements and attributes (referred to collectively as GFIPM metadata) about a federation user’s identities, privileges, and authentication can be universally communicated.

**Value to the Justice Community:**

1. **User Convenience:** Users can access multiple services using a common set of standardized security credentials, making it easier to sign on and access applications and to manage account information.
2. **Interoperability:** By specifying common security standards and framework, applications can adopt interoperable security specifications for authentication and authorization.
3. **Cost-Effectiveness:** GFIPM facilitates information sharing by using a standardized XML-based credential that includes information about each user’s identity and privileges. This reduces the cost and complexity of identity administration required to access applications and vet users.
4. **Privacy:** GFIPM can reduce the propagation of personally identifiable information, reduce the redundant capture and storage of personal identity information, and depersonalize data exchanges across domains using privacy metadata.
5. **Security:** A federation model can improve the security of local identity information and data in applications by providing a standardized approach to online identities between agencies or applications.

**Contents:** The GFIPM Governance Guidelines document defines the governance structure for a GFIPM federation, including the parties that play a role in the governance structure (e.g., Board of Directors, Federation Management Organization, Identity Provider Organizations, Service Provider Organizations, Trusted Identity Broker Organizations) and the decisions to be made by each party.

**Target Audience:** The target audience for this document includes managers and technical representatives of prospective GFIPM participant organizations who are planning to implement an Identity Provider (IDP), Trusted Identity Broker (TIB), or a Service Provider (SP) within a GFIPM federation. It also includes vendors, contractors, and consultants who are required to establish technical interoperability with GFIPM standards as part of their project or product implementation.

Table of Contents

[Acknowledgements v](#_Toc325102445)

[Document Conventions vi](#_Toc325102447)

[How to Use This Document vii](#_Toc325102448)

[1. Introduction 1](#_Toc325102449)

[2. Scope 2](#_Toc325102450)

[3. Disclaimer 3](#_Toc325102451)

[4. Core Governance Documents 4](#_Toc325102452)

[5. Board of Directors 5](#_Toc325102453)

[5.1 Composition 5](#_Toc325102454)

[5.2 Meetings of the Board of Directors 6](#_Toc325102455)

[6. Federation Governance 6](#_Toc325102456)

[6.1 Board of Directors 7](#_Toc325102457)

[6.2 Federation Management Organization 8](#_Toc325102458)

[6.3 Service Provider Organization 9](#_Toc325102459)

[6.4 Identity Provider Organization 9](#_Toc325102460)

[6.5 Trusted Identity Broker Organization 10](#_Toc325102461)

[6.6 Responsibilities of the Federation 10](#_Toc325102462)

[6.6.1 Policy 10](#_Toc325102463)

[6.6.2 Approval 10](#_Toc325102464)

[6.6.3 Suspension 11](#_Toc325102465)

[6.6.4 Audit/Investigate 11](#_Toc325102466)

[6.6.5 Revocation 11](#_Toc325102467)

[7. Systems and Security 11](#_Toc325102468)

[8. Federation Documents 12](#_Toc325102469)

[9. Personally Identifiable Information (PII) 12](#_Toc325102470)

[10. Fees and Costs 13](#_Toc325102471)

[11. Conflict Resolution 13](#_Toc325102472)

[11.1 Disputes Among Federation Members 13](#_Toc325102473)

[11.2 Disputes Between Members and the Federation Management Organization 14](#_Toc325102474)

[11.3 End User Conflict 14](#_Toc325102475)

[12. Decision to Terminate or Change the Federation 14](#_Toc325102476)

[13. Glossary 15](#_Toc325102477)

[14. References 17](#_Toc325102478)

[Appendix A—Service Provider Organization Agreement 18](#_Toc325102479)

[Appendix B—Identity Provider Organization Agreement 23](#_Toc325102493)

[Appendix C—Trusted Identity Broker Organization Agreement 28](#_Toc325102507)

[Appendix D—Document History 33](#_Toc325102520)

Acknowledgements

The Global Federated Identity and Privilege Management (GFIPM) initiative was developed through a collaborative effort of the Global Justice Information   
Sharing Initiative (Global) membership; the U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA); and the   
U.S. Department of Homeland Security (DHS). The Global Standards Council (GSC) would like to express its appreciation to BJA and DHS for their continued guidance and support of this key initiative for secure and trusted information sharing among state, regional, local, tribal, and federal organizations. The GSC would also like to thank the GFIPM Delivery Team (DT), under the direction of Mr. John Ruegg, Los Angeles County Information Systems Advisory Body, for its dedication and commitment to developing this artifact and all other companion GFIPM artifacts. The creation of this document was guided by a volunteer effort of numerous contributors who participated by leveraging GFIPM standards within their state, regional, and federal organizations. Without their subject-matter expertise, ongoing experience, and feedback from lessons learned, the development of these guidelines would not have been possible.

Document Conventions

In this document, use of a bold small-caps typeface, as in this **example**, indicates an important concept or term defined either in the glossary or in the body of the text at the point where the term or concept is first used.

In this document, use of a bold caps typeface, as in this **[example]**, indicates an important resource document that is noted in the Reference Section of this document.

How to Use This Document

It is anticipated that multiple independent Federations will be formed within and among various communities, each with their own governance structure and operational policies and procedures. Each community forming a Federation will likely customize portions of this document to meet the level of rigor required among their specific community.

Inter-federation information exchange will require common standards to be able to interoperate. This document is intended to be a model for defining Federation policies and procedures.

The content of this document has leveraged a number of industry and government standards as well as experience gained from current and ongoing pilots based on Global Federated Identity and Privilege Management (GFIPM) standards.

This document “GFIPM Operational Policies and Procedures Guidelines” [GFIPM OPP] and the companion document “GFIPM Governance Guidelines” [GFIPM GOV] correspond to the Agreement and Policy and Contract components of the Global Reference Architecture framework **[gra]** (see green components in the diagram below). These documents address the social governance roles and responsibilities for establishing and managing identity and privilege management.

The GFIPM Cryptographic Trust Model **[gfipm trust]**, GFIPM Metadata Specification Package **[gfipm metadata]**, GFIPM Web Browser User-to-System Profile **[gfipm u2s profile]**, and GFIPM Web Services System-to-System Profile **[gfipm s2s profile]** are normative GRA technical standards for a conformant GRA GFIPM Federation instance. These technical standards documents contain references to the scope of GRA components addressed. The following diagram depicts the concepts, high-level components, and relationships in the GRA Framework Version 1.9.



# Introduction

The objective of the Global Federated Identity and Privilege Management **(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. The goal of a federation is to provide justice and public safety organizations with the following benefits:

* Provide single sign-on capabilities to end users for accessing online services.
* Eliminate the requirement to register user identity information in multiple external systems.
* Retain identity management and user authentication responsibility at the local organization level.
* Provide an interoperable standard vocabulary of identity access attributes.
* Support informed access and authorization decisions based on a trusted set of user identity attributes thereby improving the security controls and scalability for justice and public safety electronic information sharing.

The federated approach to identity and privilege management provides a standards-based means for local, state, tribal, and federal entities to locally authenticate their organizations’ users and provide accurate and current user identity attributes to external justice and public safety information systems which in turn utilize the trusted attributes to make authorization and system access decisions.

Formation of a federation represents a trust model that enables local, state, tribal, federal and other justice and public-safety related entities to access online services based on the federation **attributes** issued by trusted **identity providers** (IDPs).

It is anticipated that independent federations will be formed within and among various communities, each with their own governance structure. Each community forming a federation governance structure will likely customize portions of this document to meet the level of rigor required among their specific community.

Interfederation information exchange will require common standards to interoperate. This document is intended to be a model for defining baseline capabilities and standards for forming a Federated Identity and Privilege Management governance body.

The content of this document has leveraged a number of industry and government standards as well as ongoing experience gained from current and ongoing pilots based on Global Federated Identity and Privilege Management (GFIPM) standards and guidelines.

# Scope

The purpose of this document is to identify the different parties involved in the **governance** of the [“*insert federation name*”] Federation[[1]](#footnote-1) (also referenced as “the Federation” within this document), and to define what decisions will be made by these parties. The parties involved in the governance of **the federation** are the **board of directors, federation** **management organization**, **service provider organizations**, **identity provider organizations,** and **trusted identity broker organizations.**

Definitions for these terms are given below:

**federation**: A trust model formed among a collection of Identity Provider Organizations, Service Provider Organizations, and Trusted Identity Broker Organizations spanning multiple agency organizational boundaries. Identity Provider Organizations manage the identity and authentication of their local users. Service Provider Organizations rely on Identity Provider Organizations’ assertions of attributes to make authorization and access control decisions for sharing their information. Trusted Identity Broker Organizations provide a trust bridge for certain inter-federation connections, acting on behalf of one or more Identity Provider Organizations that are not part of the Federation.

**board of directors**: This is the executive-level body with representation from primary stakeholders that guides the federation and is the final authoritative body to make decisions for the federation.

**federation management organization**: This is the body that manages the day-to-day operations of the Federation, including developing and maintaining standards, coordinating membership, and providing executive secretariat services to the Board of Directors.

**identity provider organization** (IDPO): An organizational entity that vets individuals, collects attributes about these individuals, maintains these attributes in an accurate and timely manner. The IDPO operates an **identity provider** (IDP), which is a software entity that performs user authentication each time an individual presents themselves 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.

**federation-to-federation**: The establishment of an inter-federation trust model between like and unlike federations.

**service provider** **organization** (SPO): A federation member organization that operates a **service provider** (SP), which is a software entity that provides one or more electronic information service(s) to the Federation. Service Provider Organizations’ services evaluate the set of Identity Provider attributes presented to the SP in a form that is consistent with the GFIPM Web Browser User-to-System Profile **[gfipm u2s profile]** (e.g., SAML assertion) to determine what access to provide or deny to each end user.

**trusted identity broker organization** (TIBO): A federation member organization that acts on behalf of one or more Identity Provider Organizations (IDPOs), acting as a trust bridge between those IDPOs and the Federation. A TIBO operates a Trusted Identity Broker (TIB), which is a software entity that provides the necessary cryptographic bridge and attributes translation capabilities to allow users from Identity Provider Organizations not in the Federation to access services in the Federation.

End users are not a party to the governance of the Federation. Federation policy only addresses the roles, responsibilities and commitments between Service Provider Organizations, Identity Provider Organizations, Trusted Identity Broker Organizations, and the Federation Management Organization. End user agreements for federation access are based on internal policies between the IDP or TIB and the users that it represents. Additionally, user obligations specified by a specific service policy are not in the scope of federation governance.

# Disclaimer

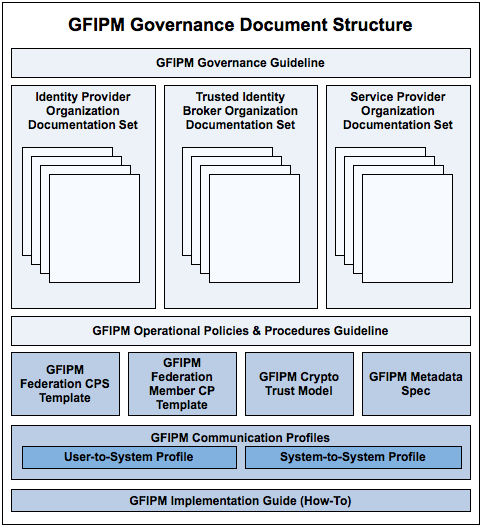
Federation governance, as defined herein, ensures that the best interests of the overall federation are maintained. It is not intended to confer any benefits or impose any obligations on the public. It neither creates nor takes away any right or benefit, substantive or procedural, enforceable at law by a party against the Service Provider Organization, Identity Provider Organization, Trusted Identity Broker Organization, the Board of Directors, the Federation Management Organization, their officers, employees or agents, local, state, tribal, or federal entities, or the public. It does not obligate, nor does it require any entity to obligate, any appropriations.

The rules of the Federation are the rules that must be maintained to stay a member of the Federation. The intent is that all parties will maintain their systems to support the trust of the other Federation members. The Federation is not liable for the actions of the individual members of the Federation.

# Core Governance Documents

The operation of the Federation is governed by the following documents, which are incorporated into this document, the Global Federated Identity and Privilege Management Governance Guidelines **[gfipm gov]**, by reference. Figure 1 illustrates the GFIPM document structure.

* GFIPM Operational Policies and Procedures Guidelines **[gfipm opp]**—this document details the way in which the Federation policies will be carried out.
* GFIPM Cryptographic Trust Model **[gfipm trust]**—this document details the technical requirements for maintaining cryptographic trust among systems in the Federation.
* GFIPM Federation Certification Practice Statement Template **[gfipm cps template]**—this document details the certification practice statement used by the Federation Management Organization in managing the cryptographic trust anchor for the Federation.
* GFIPM Federation Member Certificate Policy Template **[gfipm member cp template]**—this document details the certificate and key management policy that all Federation members must follow to ensure cryptographic trust is maintained among systems in the Federation.
* GFIPM Metadata Specification Package **[gfipm metadata]**—this specification details the metadata requirements that must be used as part of the Federation.
* GFIPM Web Browser User-to-System Profile **[gfipm u2s profile]** and GFIPM Web Services System-to-System Profile **[gfipm s2s profile]**—these documents detail the technical interfaces required to implement specific communication profiles in the Federation.



**Figure 1: GFIPM Federation Governance Document Structure**

# Board of Directors

## Composition

The Board of Directors will consist of nine representative members as listed below:

* Three standing stakeholder representatives the selection of these members will be coordinated through the Federation Management Organization.
* One representative from the Federation Management Organization—selected by the Federation Management Organization.
* Two Service Provider Organization Representatives—nominated and voted into position by the membership pool of Service Provider Organizations.
* Three Identity Provider/Broker Organization Representatives—nominated and voted into position by the membership pool of Identity Provider Organizations and Trusted Identity Broker Organizations.

## Meetings of the Board of Directors

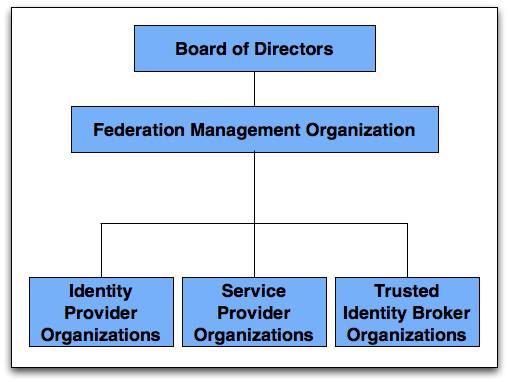
The Board of Directors shall meet regularly on a quarterly basis to discuss general business matters and other matters that may arise. On an as needed basis, the Board of Directors may call an emergency meeting to discuss and decide matters that need immediate attention. To call an unscheduled meeting, any board member must notify the other board members via written or electronic communication and obtain concurrence of no less than 50 percent of the Board to meet.

All regularly scheduled and emergency meetings shall occur in person and would require a quorum of the Board of Directors to proceed. If a quorum is not present, the meeting shall be rescheduled to the next date when a quorum may be present. Such rescheduled date shall not be more than one month from the regularly scheduled date and shall have no effect on the next regularly scheduled meeting date.

# Federation Governance

This section describes the membership roles and responsibilities and the organizational structure of a sample Federation. The governance model of the Federation is shown in Figure 2 below.

Note that the membership of the Board of Directors may be impacted by the form of federation organization. This model template governance document is based on a federation that is formed as a not-for-profit organization.



**Figure 2: GFIPM Federation Governance Model**

## Board of Directors

The role of the Board of Directors is to provide executive oversight, to decide on any matters that fall outside the role of the Federation Management Organization’s specific powers, and to provide general guidance on the day-to-day operations. This includes but is not limited to:

* Approval of any modification to the standard Identity Provider Organization, Service Provider Organization, or Trusted Identity Broker Organization Agreements (see Appendix A: Service Provider Organization Agreement, Appendix B: Identity Provider Organization Agreement, and Appendix C: Trusted Identity Broker Organization Agreement).
* Recommendation and approval of any changes to any guidelines, standards, or documents of the Federation (see Section 4 Core Governance Documents).
* Recommendation and approval of any changes to the governance structure

## Federation Management Organization

The Federation Management Organization will be responsible for the day-to-day operations of the Federation. This includes, but is not limited to, the following:

* Developing policies and guidelines pertaining to the definition and usage of the GFIPM Metadata Specification **[gfipm metadata]** standard for end-user attributes.
* Implementing approved processes for determining the membership of any new party in the Federation.
* Developing technical architecture and providing documents, including Interface Specifications, for technical interoperability within the Federation.
* Conducting day-to-day operational services, i.e., audits.
* Defining Change Management processes for the Federation.
* Conducting interoperability testing of candidate commercial products, schemes, or protocols.
* Reviewing the conformance of the applicants to membership standards, including IDPOs’ and TIBOs’ mapping of their local policies and user attributes into federation standard attributes and SPOs’ mapping of their local access control policies into Boolean logic based on federation standard attributes.
* Management and implementation of accepted federation standards and protocols operating within the Federation.
* Accountability authority and ensuring validity of the documents of the Federation.
* Facilitating the roles, relationships and mutual obligations of all parties operating in the Federation.
* Coordinate help-desk efforts and provide engineering support.
* Provide administrative support for the Board of Directors.

## Service Provider Organization

Service Provider Organizations (SPOs) provide electronic information services to users signed up with an IDPO or TIBO of the Federation. Service Provider Organizations’ services must be developed or modified to support receipt of Identity Provider Organizations’ attributes consistent with the **[gfipm u2s profile]**, (e.g., a SAML assertion from an IDP or TIB).

Upon the signing of a Service Provider Organization Agreement (See Appendix A) and approval by the Federation Management Organization, a Service Provider Organization becomes a member of the Federation. Each Service Provider Organization participates in the governance of the Federation through their ability to nominate someone from their organization or another organization to serve on the Board of Directors. Each Service Provider Organization will be allowed to submit one vote for each open Service Provider Organization Representative position on the Board of Directors.

The Service Provider Organizations may extend the **[gfipm metadata]** to meet additional attribute requirements but must provide those extensions to the Federation Management Organization for possible incorporation into future versions of the GFIPM metadata catalog.

At all times that the Service Provider Organization is a party to this agreement, it agrees to abide by the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines **[GFIPM OPP]** and the Service Provider Organization Agreement (see Appendix A).

## Identity Provider Organization

Identity Provider Organizations (IDPOs) create, maintain, and manage accurate, reliable and current identity information for end users in accordance with their published procedures. IDPs perform end-user authentication and supply the authenticated user information to SPs. The Identity Providers have a direct relationship with end users. IDPs are responsible for communicating and implementing relevant federation rules into their agreements with end users.

Upon the signing of an Identity Provider Organization Agreement (see Appendix B) and approval by the Federation Management Organization, an Identity Provider Organization is considered a member of the Federation. Each Identity Provider Organization may nominate someone from its organization or another organization to serve on the Board of Directors. Each Identity Provider Organization will be allowed to submit one vote for each open Identity Provider/Broker Organization Representative position on the Board of Directors.

At all times that the Identity Provider Organization is a party to this agreement, it agrees to abide by the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines **[gfipm opp]** and the Identity Provider Organization Agreement (see Appendix B).

## Trusted Identity Broker Organization

Trusted Identity Broker Organizations (TIBOs) act on behalf of one or more Identity Provider Organizations (IDPOs) in the case where those IDPOs have not joined the Federation but wish to make Federation services available to their users. It is important to note that even when connecting to the Federation via a TIBO, an IDPO must still provide the same level of detail about its local policies, user agreements, etc., that would be required if the IDPO joined the Federation directly. The application process for a TIBO reflects this requirement. (See **[GFIPM OPP]**.)

Upon the signing of a Trusted Identity Broker Organization Agreement (see Appendix C) and approval by the Federation Management Organization, a Trusted Identity Broker Organization is considered a member of the Federation. Each Trusted Identity Broker Organization may nominate someone from its organization or another organization to serve on the Board of Directors. Each Trusted Identity Broker Organization will be allowed to submit one vote for each open Identity Provider/Broker Organization Representative position on the Board of Directors.

At all times that the Trusted Identity Broker Organization is a party to this agreement, it agrees to abide by the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines **[GFIPM OPP]** and the Trusted Identity Broker Organization Agreement (see Appendix C).

## Responsibilities of the Federation

The responsibilities of the Federation are listed in this section.

### Policy

A membership policy for the Federation will be established by the Federation Management Organization and approved by the Board of Directors. Any subsequent changes to the policy will require the Board of Directors’ approval.

### Approval

The Federation Management Organization has the authority to approve new members and sign any Service Provider Organization Agreements, Identity Provider Organization Agreements, or Trusted Identity Broker Organization Agreements on behalf of the Federation. Any modifications to the standard agreement or assignments of these agreements will require the Board of Directors’ approval. On a periodic basis the Federation Management Organization will inform the Board of Directors of additions and removals to membership.

### Suspension

Suspension of membership may occur for cause or suspicion of cause. The Federation Management Organization may suspend membership for up to 15 days; a longer suspension may be imposed by the Board of Directors.

### Audit/Investigate

The Federation has the right to audit the federation-related activities of any member across the Federation. In the case of an alleged breach of federation policy, the Federation can perform basic audit and investigation. If there is initial validation of the concern based on the initial investigation, the member can be required to provide third-party audit to show that their procedures adhere to federation rules.

### Revocation

Revocation for cause must follow the complaint process in the GFIPM Operational Policies and Procedures Guidelines **[GFIPM OPP],** and final decision to revoke an IDP or SP must be approved by the Board of Directors. If suspicion exists that an IDP or SP has violated any of the Federation provisions, standards, policies, or procedures contained in the Federation documents and that violation threatens the integrity of the Federation, then the Federation Management Organization or Board of Directors may temporarily suspend the IDP or SP under suspicion while the suspicion is investigated. If the suspicion is proven, then the Federation Management Organization will make a recommendation to the Board of Directors to either allow the violating IDP or SP to cure the violation or to revoke their membership.

The decision to revoke any member’s membership without cause will be in the sole discretion of the Board of Directors and will require 60 days notice to such member. If any member decides to cancel their membership, they may do so upon 60 days notice to the Federation Management Organization. The Federation Management Organization will be responsible for periodically informing the Board of Directors of the cancellation of any memberships.

# Systems and Security

All of the Federation technical and security policies, processes, guidelines, and standards will be documented for the membership. These documents and the evaluation of the ongoing federation systems will be maintained by the Federation Management Organization or its designee.

Any non-urgent operational issues that arise regarding the systems or security will be researched by the Federation Management Organization and if it is determined that a change to the system or security may be required, the Federation Management Organization will make a recommendation for this change to the Board of Directors, and the Board of Directors may either approve or deny the change to the system or security.

Any urgent issues regarding the systems or security that arise may be resolved, mitigated, or addressed immediately by the Federation Management Organization. The Federation Management Organization will notify the Board of Directors immediately of the urgent issue that arose and its resolution of the matter. The Federation Management Organization has the responsibility to alert the party responsible for the security and notification of risk to the rest of the federation members and to follow the appropriate alert procedures as described in the GFIPM Operational Policies and Procedures Guidelines **[gfipm opp]**. The Board of Directors must ratify the change or ask the Federation Management Organization to propose a different resolution acceptable to the Board of Directors within 15 days. The Federation Management Organization will be given adequate time to implement any alternative solutions.

# Federation Documents

All of the Federation’s policies, processes, system requirements, security requirement, software requirements, and governance decisions will be detailed in the documents listed in Section 4 of this document (see Core Governance Documents, p. 3). Once the Board of Directors is formally established, it will approve the final drafts of these documents. Any changes to the Federation’s documents will require approval of the Board of Directors.

# Personally Identifiable Information (PII)

The intent of the Federation is to improve information sharing and in order to do that in a responsible manner, all IDPs and SPs must manage identity attributes to ensure the safeguarding of personal data. Service Provider Organizations are required to handle all Identity Provider Organizations’ **personally identifiable information (pii)** in accordance with the Federation’s policies. Identity Provider Organizations assert identity attribute data, including PII attributes, as necessary to meet the authorization requirements of Service Provider Organizations, for audit logs and for supporting dynamic account provisioning. IDPO attributes, including PII attributes, shall not be used for any other business purposes.

# Fees and Costs

The Federation may charge management fees to allow for the costs of the Federation upkeep and coordination. The fees will be kept to a minimum by requiring members to fund the following activities:

* Development of their own policy documents.
* Providing Tier 1 Help Desk support to their own end customers and Tier 2 support for the IDPs.
* Perform required auditing on a timely basis.

# Conflict Resolution

The Federation members agree that any dispute, claim action, or suit between them will first be brought to the Federation for resolution, before bringing any dispute, claim, action, or suit before a court of law, as described below. All decisions made by the Board of Directors in resolution of a conflict will be deemed final upon notice to the parties involved. Unless otherwise stipulated in the resolution description, the decision will be implemented in 30 days from initial notice.

## Disputes Among Federation Members

Disputes among the Federation members shall be resolved via the following process. When a dispute occurs among members, one or more members may notify the Federation Management Organization of the dispute in writing. Upon receiving written notification of the dispute, the Federation Management Organization may, at its discretion, take the necessary steps to investigate the dispute. After investigating the dispute, the Federation Management Organization may either render a decision to resolve the dispute or submit the issue to the Board of Directors for a vote. The Federation Management Organization must complete this process no later than 60 days after receiving written notification of the dispute.

## Disputes Between Members and the Federation Management Organization

Disputes between Federation members and the Federation Management Organization shall be resolved via the following process. When a dispute occurs between any of the Federation members and the Federation Management Organization, one or more parties to the dispute may notify the Board of Directors of the dispute in writing. Upon receiving written notification of the dispute, the Director in receipt of the written notification must forward the notification to all members of the Board of Directors. The Board of Directors may, at its discretion, take the necessary steps to investigate and render a decision on the dispute. The Board of Directors must complete this process no later than 60 days after receiving written notification of the dispute.

## End User Conflict

Any end-user conflict will be addressed solely by the Identity Provider Organization to which the user subscribes, and cannot be appealed to any other federation member.

# Decision to Terminate or Change the Federation

The Board of Directors will have the sole discretion to terminate the Federation. When making the decision to terminate the Federation, the Board of Directors must give at least 120 days notice to all members of the Federation and provide a documented process for the termination of the Federation to all members.

# Glossary

**Attributes**

Professional characteristics of a user that have been verified by an IDP which will allow that individual to access particular sets of services provided by an SP.

**Board of Directors**

The Board of Directors decides on any matters that fall outside of the role of the Federation Management Organization and provide general guidance. Some of the responsibilities include approval of any modification to standard agreements, documents, or governance structure.

**Federation Management Organization**

The Federation Management Organization is responsible for the day-to-day operations of the Federation.

**Governance**

Establishment of policies and continuous monitoring of the proper implementation by the members of the governing body of an organization.

**Identity Provider Organization**

An organizational entity that manages users and user identities is called an Identity Provider Organization (IDPO). An Identity Provider Organization conveys information about an end user to a Service Provider Organization and performs basic user management tasks such as vetting, credentialing, and authentication.

**Personally Identifiable Information (PII)**

Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

**Service Provider Organization**

An organizational entity that manages resources is called a Service Provider Organization (SPO). An SPO maintains complete control of its resources and performs basic resource management tasks, including definition and enforcement of resource access requirements and access control policies.

**Trusted Identity Broker Organization**

An organizational entity that acts on behalf of one or more Identity Provider Organizations (IDPO) in the case where the IDPO has not joined the Federation, but wishes to make Federation services available to its users, is called a Trusted Identity Broker Organization (TIBO). A TIBO acts as an organizational trust bridge between one or more non-Federation member IDPO and one or more Federation member SPO.

# References

Note: Some of the following deliverables are in working draft form and will be published on the OJP Web site (see <http://it.ojp.gov>) in the near future.

GFIPM OPP Global Standards Council. Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines, Version 1.1, May 31, 2012.

GFIPM Trust Global Standards Council. Global Federated Identity and Privilege Management Cryptographic Trust Model, Version 2.0,   
May 31, 2012.

GFIPM Member CP Template Global Standards Council. Global Federated Identity and Privilege Management Federation Member Certificate Policy Template, Draft Version, Not Yet Published.

GFIPM CPS Template Global Security Working Group. Global Federated Identity and Privilege Management Federation Certification Practice Statement Template, Version 1.0, September 14, 2010.

GFIPM Metadata Global Security Working Group. Global Federated Identity and Privilege Management Metadata Specification, Version 2.0,   
September 14, 2010.

**GFIPM U2S Profile** Global Standards Council. Global Federated Identity and Privilege Management Web Browser User-to-System Profile, Version 1.2, May 31, 2012.

**GFIPM S2S Profile** Global Standards Council. Global Federated Identity and Privilege Management Web Services System-to-System Profile, Draft Version. Not Yet Published.

Appendix A—Service Provider Organization Agreement

In order to allow for the connection of multiple parties in an electronic information sharing trust environment, The **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*insert federation name*)** Federation (“the Federation”) allows for the interconnection of separately provided identities, associated with end users, and services for those users.

Therefore,

# Preamble

This Service Provider Organization Agreement (the “SPO Agreement”) is being entered into by the Federation Management Organization and **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*insert authorized organization name*)**, the Service Provider Organization. The purpose of the SPO Agreement is to memorialize the intent of the Service Provider Organization to provide services to the Federation and for the Federation Management Organization to allow the Service Provider Organization access to the Federation infrastructure to unite Identity Provider Organization end-users and the Service Provider Organization’s services.

# Service Provider Organization Role

The Service Provider Organization 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 Organization end-users who meet the requirements of an established and documented access policy that the Service Provider Organization has defined.

Unless the Service Provider Organization has specifically identified certain or all of the Service Provider Organization’s services as not public, the Federation may publicize the services that the Service Provider Organization has made available to the Federation. However, Service Provider Organizations who need to keep confidential the availability of their service(s) may specify the set of required attributes for discovery of their services in the Federation directory of services.

At all times that the Service Provider Organization is a party to this agreement, it agrees to abide by **[gfipm opp]**. Specifically the Service Provider Organization agrees to meet minimum security and availability standards.

The Service Provider Organization agrees to comply with any decisions made through the governance process, in accordance with the Global Federated Identity and Privilege Management Governance Guidelines **[gfipm gov]**.

1. Service Provider Organizations shall have the capability to validate identity assertions that are submitted by the Federation Identity Provider Organizations (IDPOs) as part of a service request.
2. Service Provider Organizations shall have the ability to define attributes that IDPOs must present for access to the service.
3. Service Provider Organizations shall have the capability to react to receipt of various requestor assertions based on the established policy.
4. Service Provider Organizations shall provide audit services and make them available upon request to the federation.

All Service Provider Organizations must certify that they are only providing information or services that they have legal rights to provide.

Consumers of a federation service are obligated to comply with the specific service-level policies governing the appropriate use, handling, dissemination, and/or destruction of the information accessed. The user obligations specified by a specific service policy are not in the scope of the Federation governance.

# Federation Role

The Federation Management Organization agrees that it will provide the Service Provider Organization with the operational support to enable the Identity Provider Organizations’ end-users and the Service Provider Organization’s services to interact. The Federation Management Organization agrees that it will abide by the Federated Identity and Privilege Management Operational Policies and Procedures Guidelines **[gfipm opp]** and that it will make governance decisions in accordance with GFIPM Governance Guidelines **[gfipm gov]**.

# Personally Identifiable Information

All Service Provider Organizations must manage their information service privacy data in accordance with their service-specific privacy policies. All identity attributes received by the Service Provider Organization from Identity Provider Organizations can only be used to make authorization decisions, dynamically provision accounts, and perform audit logging.

# Termination

Termination of this agreement may occur for cause or for no cause. Either party may terminate this agreement, in accordance with the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines **[gfipm opp],** upon the occurrence of any material default of this agreement by the other party or upon 60 days notice to the other party.

# Modification of Agreement

A modification of this agreement proposed by the Federation Management Organization or by the Service Provider Organization will not be final unless it has been agreed to by both parties and approved by the Board of Directors in writing.

# Waiver

A waiver of any provision of this agreement shall not be considered a permanent waiver of such provision unless agreed to in writing by the Federation Management Organization and the Board of Directors.

# Assignment

This agreement may not be assigned, in whole or in part, by the Service Provider Organization without the prior written consent of the Federation Management Organization and the Board of Directors.

# Severability

If any provision of this Agreement is vague or contradicts another provision in this agreement or any Federation Document, the remaining provisions of this Agreement nevertheless will continue in full force and effect without being impaired or invalidated in any way. The vague or contradictory provision will be reviewed and then clarified or corrected by the Board of Directors.

# Entire Agreement

This Agreement is the entire Agreement between the parties and supersedes any and all prior oral and written agreements, commitments, understandings or communications with respect to the subject matter of this Agreement. This Agreement may not be modified except in writing and signed by a duly authorized representative of each party.

# Federation Documents

The operation of the Federation is governed by the following documents, which are incorporated into this agreement by reference:

* The Global Federated Identity and Privilege Management Governance Guidelines **[gfipm gov]—**this document defines the roles and responsibilities of the Federation, the Federation Management Organization, the Board of Directors, Service Provider Organizations, Identity Provider Organizations, and Trusted Identity Broker Organizations.
* The Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines **[gfipm opp]**—this document details the way in which the Federation policies will be carried out.
* GFIPM Cryptographic Trust Model **[gfipm trust]**—this document details the technical requirements for maintaining cryptographic trust among systems in the Federation.
* GFIPM Federation Certification Practice Statement Template **[gfipm cps template]**—this document details the certification practice statement used by the Federation Management Organization in managing the cryptographic trust anchor for the Federation.
* GFIPM Federation Member Certificate Policy Template **[gfipm member cp template]**—this document details the certificate and key management policy that all Federation members must follow to ensure cryptographic trust is maintained among systems in the Federation.
* GFIPM Metadata Specification **[gfipm metadata]**—this specification details the metadata requirements that must be used as part of the Federation.
* GFIPM Web Browser User-to-System Profile **[gfipm u2s profile]** and GFIPM Web Services System-to-System Profile **[gfipm s2s profile]**—these documents detail the technical interfaces required to implement specific communication profiles in the Federation.

# Notices

All notices, certificates, acknowledgments, or other written communications required to be given under this Agreement shall be in writing and shall be deemed to have been given and properly delivered if duly mailed by certified or registered mail to the other Party at its address as follows, or to such other address as either Party may, by written notice, designate to the other.

Notice to the Federation Management Organization shall be delivered as follows:

***\_\_\_\_\_\_(insert address)***

Notice to the Service Provider Organization shall be delivered as follows:

***\_\_\_\_\_\_(insert address)***

The following material, which has been submitted with this agreement, is incorporated in the agreement by reference:

**(*insert list documents*)**

# Signature

By signing below **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*insert authorized organization name)***, the Service Provider Organization, certifies that they have read this document, that it is accurate, and agrees to abide by this agreement and all Federation documents referenced herein.

|  |  |
| --- | --- |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*insert authorized organization name*)**, the Service Provider Organization  By: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(signature of authorized representative)***  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*insert title)*** |  |

Appendix B—Identity Provider Organization Agreement

In order to allow for the connection of multiple parties in an electronic information sharing trust environment, the **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*insert federation name*)** Federation “the Federation”) allows for the interconnection of separately provided identities, associated with end users, and services for those users.

# Preamble

This Identity Provider Organization Agreement (the “IDPO Agreement”) is being entered into by the Federation Management Organization and **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*insert* *authorized organization name)***, the Identity Provider Organization. The purpose of the IDPO Agreement is to memorialize the intent of the Federation Management Organization to provide access to the federation systems to Identity Provider Organization and its end users, and for the Identity Provider Organization to create, maintain, and manage identities of their respective end users.

# Identity Provider Organization Role

The role of the Identity Provider Organization is to create, maintain, secure, and manage the identities of their end users and accurately assert those identities and attributes about those identities only to authorized Federation Service Provider Organizations (SPOs) in accordance with federation technical documents. In accomplishing this role, the Identity Provider Organization agrees that it will adhere to a documented process for the initial vetting of their end-users identities for any changes, for the removal of end users, and for the ongoing management of users attributes.

At all times that the Identity Provider Organization is a party to this agreement, it agrees to abide by the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines **[gfipm opp].**  Specifically, the Identity Provider Organization agrees to meet minimum security and availability standards and at a minimum shall do the following:

1. Identity Provider Organization shall provide a trust model that ensures that an individual is linked to identities that have been issued, protected, and managed to provide the accuracy of asserted attributes.
2. Identity Provider Organization shall develop and provide an authentication process by which the user provides evidence to the Identity Provider Organization, which independently verifies that the user is who he or she claims to be.
3. Identity Provider Organization shall develop a process to periodically reevaluate the status of the user and the validity of his or her associated identity.
4. Identity Provider Organization shall develop a process for attribute management to ensure the timely cancellation or modification of attributes should the user’s status change.
5. Identity Provider Organization shall develop a process for auditing the attribute identification process, including registration activities, to ensure attributes are maintained in accordance with the process specified by that Identity Provider Organization. Auditing must be conducted in a manner to identify any irregularities or security breaches. Audit information must be made available to the federation upon request.
6. Identity Provider Organization shall provide a process to assist users who have either lost or forgotten their means of authentication.
7. Identity Provider Organization shall adhere to the problem resolution process in Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines **[gfipm opp]**.

# Federation Role

The Federation Management Organization agrees that it will provide the Identity Provider Organization and its end users access to the federation systems. The Federation Management Organization agrees that it will abide by the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines **[gfipm opp]** and that it will make governance decisions in accordance with the Federated Identity and Privilege Management Governance Guidelines **[gfipm opp]**.

# Personally Identifiable Information (PII)

Identity Provider Organizations assert identity attribute data, including PII attributes, as necessary to meet the authorization requirements of Service Provider Organizations, for audit logs and for supporting dynamic account provisioning. IDP attributes, including PII attributes, shall not be used for any other business purposes.

# Termination

Termination of this agreement may occur for cause or for no cause. Either party may terminate this agreement, in accordance with the Global Federated Identity and Privilege Management Operational Policies and Procedures **[GFIPM OPP]**, upon the occurrence of any material default of this agreement by the other party or upon 60 days notice to the other party.

# Modification of Agreement

A modification of this agreement proposed by the Federation Management Organization or by the Identity Provider Organization will not be final unless it has been agreed to by both parties and approved by the Board of Directors in writing.

# Waiver

A waiver of any provision of this agreement shall not be considered a permanent waiver of such provision unless agreed to in writing by the Federation Management Organization and the Board of Directors.

# Assignment

This agreement may not be assigned, in whole or in part, by the Identity Provider Organization without the prior written consent of the Federation Management Organization and the Board of Directors.

# Severability

If any provision of this Agreement is vague or contradicts another provision in this agreement or any Federation Document, the remaining provisions of this Agreement nevertheless will continue in full force and effect without being impaired or invalidated in any way. The vague or contradictory provision will be reviewed and then clarified or corrected by the Board of Directors.

# Entire Agreement

This Agreement is the entire Agreement between the parties and supersedes any and all prior oral and written agreements, commitments, understandings or communications with respect to the subject matter of this Agreement. This Agreement may not be modified except in writing and signed by a duly authorized representative of each party.

# Federation Documents

The operation of this Federation is governed by the following documents, which are incorporated into this agreement by reference:

* The Global Federated Identity and Privilege Management Governance Guidelines **[gfipm gov]**—this document defines the roles and responsibilities of the Federation, the Federation Management Organization, the Board of Directors, Service Provider Organizations, Identity Provider Organizations, and Trusted Identity Broker Organizations.
* Global Federated Identity and Privilege Management Operational Standards Policies and Procedures Guidelines **[gfipm opp]**—this document details the way in which the federation policies will be carried out.
* GFIPM Cryptographic Trust Model **[gfipm trust]**—this document details the technical requirements for maintaining cryptographic trust among systems in the Federation.
* GFIPM Federation Certification Practice Statement Template **[gfipm cps template]**—this document details the certification practice statement used by the Federation Management Organization in managing the cryptographic trust anchor for the Federation.
* GFIPM Federation Member Certificate Policy Template **[gfipm member cp template]**—this document details the certificate and key management policy that all Federation members must follow to ensure cryptographic trust is maintained among systems in the Federation.
* GFIPM Metadata Specification **[gfipm metadata]**—this specification details the metadata requirements that must be used as part of the Federation.
* GFIPM Web Browser User-to-System Profile **[gfipm u2s profile]** and GFIPM Web Services System-to-System Profile **[gfipm s2s profile]**—these documents detail the technical interfaces required to implement specific communication profiles in the Federation.

# Notices

All notices, certificates, acknowledgments or other written communications required to be given under this Agreement shall be in writing and shall be deemed to have been given and properly delivered if duly mailed by certified or registered mail to the other Party at its address as follows, or to such other address as either Party may, by written notice, designate to the other.

Notice to the Federation Management Organization shall be delivered as follows:

**\_\_\_\_(*Insert address*)**

Notice to the Identity Provider Organization shall be delivered as follows:

**\_\_\_\_(*Insert address*)**

The following material, which has been submitted with this agreement, is incorporated in the agreement by reference:

***(List documents)***

# Signatures

By signing below **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, (*authorized organization name)***, the Identity Provider Organization, certifies that they have read this document, that it is accurate, and agrees to abide by this agreement and all Federation documents referenced herein.

|  |
| --- |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*authorized organization name)***, the Identity Provider Organization  By: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*authorized representative)***  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (title*)*** |

Appendix C—Trusted Identity Broker Organization Agreement

A Trusted Identity Broker Organization (TIBO) provides security token translation services from one federation domain of Identity Provider Organizations (IDPOs) and their respective Identity Providers (IDPs) to another federation domain. A Trusted Identity Broker (TIB) is a security service gateway that provides one-way or two-way transmission of identity credentials and attributes between federations.

# Preamble

This Trusted Identity Broker Organization Agreement (the “TIBO Agreement”) is being entered into by the Federation Management Organization and \_\_\_\_\_\_\_\_\_\_\_, the Trusted Identity Broker Organization (TIBO). The purpose of the TIBO Agreement is to memorialize the intent of the Federation Management Organization to provide access to Federation systems via the TIBO and its collective set of IDPs’ end users.

# Trusted Identity Broker Organization Role

The role of the TIBO is to perform two basic tasks.

1. Vet brokered IDPOs and their identity providers (IDPs).
2. Establish a secure connection to each IDP and translate and generate user assertions from each IDPO that accurately asserts those identities, and attributes about those identities, to authorized Federation Service Providers in accordance with Federation technical documents.

In accomplishing this role, the TIBO agrees that it will adhere to a documented process for the initial vetting of its IDPOs and provide updates to any changes in IDPOs that would amend the original onboarding documentation.

At all times that the TIBO is a party to this agreement, it agrees to abide by the Federation Policies and Procedures Document. Specifically, the TIBO agrees to meet minimum security and availability standards and, at a minimum, shall do the following:

1. The TIBO shall provide a trust model that ensures that an individual is linked to identities that have been issued, protected, and managed to provide the accuracy of asserted attributes.
2. The TIBO shall develop and provide an authentication process by which the user provides evidence to the TIBO, which independently verifies that the user assertion is from one of the TIBO’s vetted IDPOs.
3. The TIBO shall develop a process to periodically require its IDPOs to evaluate the status of their users and the validity of their associated identities.
4. The TIBO shall review its IDPOs’ processes for attribute management to ensure the timely cancellation or modification of attributes should the user’s status change.
5. The TIBO shall develop a process for auditing each vetted IDPO’s attribute identification process, including registration activities, to ensure that attributes are maintained in accordance with the process specified by the TIBO. Auditing must be conducted in a manner to identify any irregularities or security breaches. Auditing must be made available to the Federation upon request.
6. The TIBO shall verify that its IDPOs have a process to assist users who have either lost or forgotten their means of authentication.
7. The TIBO shall adhere to the problem resolution process in the Policies and Procedures document.

# Federation Role

The Federation Management Organization agrees that it will provide the TIBO and its IDPOs’ end users access to the Federation systems. The Federation Management Organization agrees that it will abide by the Federation Policies and Procedures Document and that it will make governance decisions in accordance with the Federation Governance Document.

# Termination

Termination of this agreement may occur for cause or for no cause. Either party may terminate this agreement, in accordance with the Federation Policies and Procedures Document, upon the occurrence of any material default of this agreement by the other party or upon 60 days notice to the other party.

# Modification of Agreement

A modification of this agreement proposed by the Federation Management Organization or by the TIBO will not be final unless it has been agreed to by both parties and approved by the Advisory Board in writing.

# Waiver

A waiver of any provision of this agreement shall not be considered a permanent waiver of such provision unless agreed to in writing by the Federation Management Organization and the Advisory Board.

# Assignment

This agreement may not be assigned, in whole or in part, by the TIBO without the prior written consent of the Federation Management Organization and the Advisory Board.

# Severability

If any provision of this Agreement is vague or contradicts another provision in this agreement or any Federation Document, the remaining provisions of this Agreement nevertheless will continue in full force and effect without being impaired or invalidated in any way. The vague or contradicting provision will be reviewed and then clarified or corrected by the Advisory Board.

# Entire Agreement

This Agreement is the entire Agreement between the parties and supersedes any and all prior oral and written agreements, commitments, understandings or communications with respect to the subject matter of this Agreement. This Agreement may not be modified except in writing and signed by a duly authorized representative of each party.

# Federation Documents

The operation of this Federation is governed by the following documents, which are incorporated into this agreement by reference:

* The Global Federated Identity and Privilege Management Governance Guidelines **[gfipm gov]**—this document defines the roles and responsibilities of the Federation, the Federation Management Organization, the Board of Directors, Service Provider Organizations (SPOs), Identity Provider Organizations (IDPOs), and Trusted Identity Broker Organizations (TIBOs).
* Global Federated Identity and Privilege Management Operational Standards Policies and Procedures Guidelines **[gfipm opp]**—this document details the way in which the Federation policies will be carried out.
* GFIPM Cryptographic Trust Model **[gfipm trust]**—this document details the technical requirements for maintaining cryptographic trust among systems in the Federation.
* GFIPM Federation Certification Practice Statement Template **[gfipm cps template]**—this document details the certification practice statement used by the Federation Management Organization in managing the cryptographic trust anchor for the Federation.
* GFIPM Federation Member Certificate Policy Template **[gfipm member cp template]**—this document details the certificate and key management policy that all Federation members must follow to ensure cryptographic trust is maintained among systems in the Federation.
* GFIPM Metadata Specification **[gfipm metadata]**—this specification details the metadata requirements that must be used as part of the Federation.
* GFIPM Web Browser User-to-System Profile **[gfipm u2s profile]** and GFIPM Web Services System-to-System Profile **[gfipm s2s profile]**—these documents detail the technical interfaces required to implement specific communication profiles in the Federation.

# Notices

All notices, certificates, acknowledgments or other written communications required to be given under this Agreement shall be in writing and shall be deemed to have been given and properly delivered if duly mailed by certified or registered mail to the other Party at its address as follows, or to such other address as either Party may, by written notice, designate to the other.

Notice to the Federation Management Organization shall be delivered as follows:

**\_\_\_\_(*Insert address*)**

Notice to the Trusted Identity Broker Organization shall be delivered as follows:

**\_\_\_\_(*Insert address*)**

The following material, which has been submitted with this agreement, is incorporated in the agreement by reference:

***(List documents)***

# Signatures

By signing below \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, the Trusted Identity Broker Organization, certifies that they have read this document, that it is accurate, and agrees to abide by this agreement and all Federation documents referenced herein.

|  |
| --- |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*authorized organization name)***, the Trusted Identity Broker Organization  By: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*authorized representative)***  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (title*)*** |

Appendix D—Document History

| **Date** | **Version** | **Editor** | **Change** |
| --- | --- | --- | --- |
| September 30, 2008 | 0.8 | Patricia Hammar | Initial draft |
| September 14, 2010 | 1.0 | Matt Moyer | Final edits for version 1.0 |
| May 26, 2011 | 1.1 | Matt Moyer | Added TIBO concept;  clarified IDP vs. IDPO and SP vs. SPO. |
| April 12, 2012 | 1.1 | Global Standards Council (GSC), Global Federated Identity and Privilege Management Delivery Team (GFIPM DT) | Approved |

BACK COVER—

About Global 
The 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 Global and its products, including those referenced in this document, call (850) 385-0600 or visit http://www.it.ojp.gov/GIST.

About GSC 
In accordance with the founding principle of Global, the Global Standards Council (GSC) directly supports the broadscale exchange of pertinent justice and public safety information by promoting standards-based electronic information exchanges for the justice community as a whole.  Specifically, the GSC develops, maintains, and sustains the standards—including this particular standard—associated with these aforementioned information exchanges.  To further foster community participation and reuse, the GSC also receives, evaluates, and recommends to Global for adoption proposed standards submitted by Global consumers and stakeholders.   In turn, the GSC employs an enterprise architecture approach for developing and maintaining the cohesive body of Global standards as one Global Standards Package (GSP), which can be accessed at http://www.it.ojp.gov/gsp.

BJA Disclaimer
This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice, 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.


1. One operational example is the National Information Exchange Federation. [↑](#footnote-ref-1)