FRONT COVER—

Federated Identity and Privilege Management, Operational Policies and Procedures 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
The collection of Global-recommended normative standards has been developed and assembled into a unified package of composable, interoperable solutions that enable effective information exchange.  The collection is known as the Global Standards Package (GSP).  GSP solutions are generally focused on resolving technical interoperability challenges but also may include associated guidelines and operating documents to assist implementers.  The GSP includes 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 are reusable nationwide in order to save time and money and reduce complexity when implementing particular information exchanges with external partners.
•  Global Federated Identity and Privilege Management (GFIPM):  Guidelines and standards for establishing, implementing, and governing security, identity management, and access control solutions to ensure that information can be accessed only securely and appropriately. 
•  Global Privacy Technology Framework:  A framework for automating information access controls based on privacy and related policies restricting the use of dissemination of such information.

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 Operational Policies and Procedures Guidelines document describes the operational policies and procedures that govern the basic operation of a federation for trusted information sharing, including federation membership, change management for federation standards, help desk policies, etc. It also contains some normative language related to operational protocol between parties in the federation.

**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), Service Provider (SP), or Trusted Identity Broker (TIB) role 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 iv](#_Toc325120230)

[How to Use This Document v](#_Toc325120231)

[Document Conventions vii](#_Toc325120233)

[1. Introduction 1](#_Toc325120234)

[2. Federation Document Structure 2](#_Toc325120235)

[3. Out of Scope 4](#_Toc325120236)

[4. Compliance With Federation Policies and Procedures 5](#_Toc325120237)

[4.1 Definitive Authority 5](#_Toc325120238)

[4.2 Notation and Compliance With Normative Language 5](#_Toc325120239)

[5. Federation Membership Processes 5](#_Toc325120240)

[5.1 Request-to-Join Process 6](#_Toc325120241)

[5.2 Application Process 7](#_Toc325120242)

[5.3 Onboarding Process 12](#_Toc325120243)

[5.4 Ongoing Membership 13](#_Toc325120244)

[6. Change Management for Normative Standards 14](#_Toc325120245)

[6.1 Process for Proposing Changes 15](#_Toc325120246)

[6.2 Process for Reviewing and Responding to Suggestions 15](#_Toc325120247)

[6.3 Submission of Vetted Changes to Global 15](#_Toc325120248)

[7. Management of Federation Help Desk Services 15](#_Toc325120249)

[8. Other Considerations for Information Sharing Federations 17](#_Toc325120250)

[9. Glossary 18](#_Toc325120251)

[10. References 19](#_Toc325120252)

[Appendix A—Application to Join the Federation 21](#_Toc325120253)

[Appendix B—Request to Join as a Service Provider Organization 22](#_Toc325120254)

[Appendix C—Request to Join as an Identity Provider Organization 23](#_Toc325120255)

[Appendix D—Request to Join as a Trusted Identity Broker Organization 24](#_Toc325120256)

[Appendix E—Implementation Documentation Form for a Service Provider 26](#_Toc325120257)

[Appendix F—Implementation Documentation Form for an Identity Provider 27](#_Toc325120258)

[Appendix G—Implementation Documentation Form for a Trusted Identity Broker 28](#_Toc325120259)

[Appendix H—GFIPM Member Security Practices Checklist 29](#_Toc325120260)

[Appendix I—Document History 33](#_Toc325120261)

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.

How to Use This Document

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 (GRA) framework (see green components in the diagram below). These documents address the social governance roles and responsibilities for establishing and managing identity and privilege management.

It is anticipated that multiple independent federations will be formed within and among various communities, each with its 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 within its purview.

Interfederation information exchange will require common standards.

This document leverages 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. It is intended to be a model for defining federation policies and procedures.

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 GRA components that are addressed. The following diagram depicts the concepts, high-level components, and relationships in the GRA Framework Version 1.9.

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.

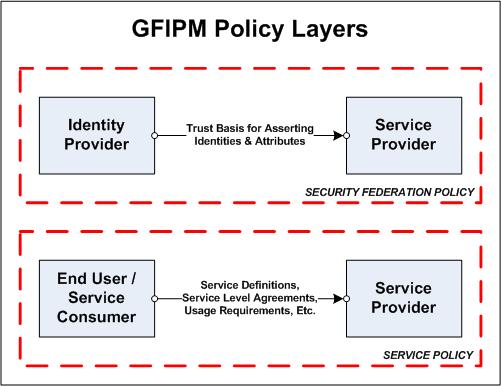
In this document, use of a bold caps typeface, as in this **[example]**, indicates an important resource document that is noted in the Reference Section of this document.

# 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 security identity 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 purpose of this document is to describe 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. Figure 1 below illustrates the two fundamental policy layers that facilitate secure information sharing within a GFIPM-based federation. The focus of this document is to establish and facilitate the necessary base policies and procedures to provide trust relationships for the purpose of federated identity and privilege management among federation members at the security federation policy layer. Some members may have additional service-level policy requirements that need to be layered on top of the base federation agreements and policies. While complementary with the GFIPM governance and approach, those policies, processes, and procedures are considered outside the scope of this document.



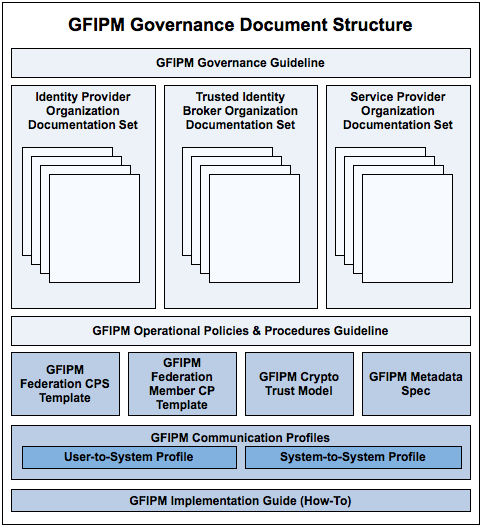
**Figure 1: GFIPM Federation Policy Layers**

The target audience for this document includes representatives of prospective federation participants who intend to join the federation as an Identity Provider Organization (IDPO), Service Provider Organization (SPO), Trusted Identity Broker Organization (TIBO), or some combination of these roles, as well as current members.

These guidelines serve as a working draft. It is anticipated that this document will continue to evolve and mature over time as the GFIPM concept matures and participants gain more experience with the issues surrounding federation governance.

# Federation Document Structure

One of the fundamental lessons learned during the GFIPM Security Interoperability Demonstration Project **[gfipm demonstration]**,which was funded by the U.S. Department of Homeland Security, was that the ultimate success of any information sharing federation would depend critically on the existence of a solid governance structure and a set of operational policies and procedures under which the federation can operate. Toward this end, a set of federation governance documents, including this document, was developed for the GFIPM initiative. Figure 2 illustrates the complete set of GFIPM federation documents relating to governance, operations, and technical standards.



**Figure 2: GFIPM Governance Document Structure**

As illustrated in Figure 2 above, the GFIPM federation governance and technical document structure consists of the following documents.

* Global Federated Identity and Privilege Management Governance Guidelines **[gfipm gov]**—Details the way in which the federation policies will be carried out, and it defines the federation governance structure, including participants, roles, and procedures for changing federation rules and policies.
* Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines **[gfipm opp]**—Details the way in which the federation policies will be carried out. This guideline includes as attachments the various documents necessary for becoming a federation member:
  + Application Form (see Appendix)
  + Identity Provider Organization Documentation Package—Information package submitted by each Identity Provider Organization (IDPO) in the federation.
  + Service Provider Organization Documentation Package—Information package submitted by each Service Provider Organization (SPO) in the federation.
  + GFIPM Member Security Practices Checklist (see Appendix)
* 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 (FMO) 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.
* GFIPM Implementation Guide—Provides technical implementation guidance for participants.

# Out of Scope

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. Note that by definition, this does not include policies and procedures relating to the Service Provider information content that is exchanged within the federation. Information content policies such as service level agreements and usage agreements fall outside the scope of this document. Although service specific usage policy and information handling is critical to the goal of information sharing, those service-level definitions are not in the scope of federation policy for an interorganizational identity and access control trust model.

# Compliance With Federation Policies and Procedures

## Definitive Authority

This document is the definitive authority on all Federation Operational Policies and Procedures. It incorporates by reference the following other documents.

|  |  |
| --- | --- |
| **Document ID** | **Document Name** |
| [GFIPM GOV] | GFIPM Governance Guidelines |
| [GFIPM TRUST] | GFIPM Cryptographic Trust Model |
| [GFIPM CPS TEMPLATE] | GFIPM Federation Certification Practice Statement Template |
| [GFIPM MEMBER CP TEMPLATE] | GFIPM Federation Member Certificate Policy Template |
| [GFIPM METADATA] | GFIPM Metadata Specification Version 2.0 |
| [GFIPM U2S PROFILE] | GFIPM Web Browser User-to-System Profile |
| [GFIPM S2S PROFILE] | GFIPM Web Services System-to-System Profile |

**Table 1:** Document References for GFIPM-specific Standards

## Notation and Compliance With Normative Language

Portions of this document contain normative language including the key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL.” Any occurrences of these words in this document are to be interpreted as described in [RFC 2119]. All federation participants, including members and the Federation Management Organization (FMO), must comply with the normative portions of this document.

# Federation Membership Processes

To ensure that appropriate trust exists among federation members for the conduct of information sharing activities, the federation shall adhere to the processes defined herein regarding membership.

An organization wishing to participate in the federation MUST adhere to the following sequence of membership phases and associated processes:

1. Request-to-Join Process
2. Application Process
3. Onboarding Process
4. Ongoing Membership

Figure 3 illustrates this sequence of phases, and sections 5.1 through 5.4 define each phase and its associated process and requirements.

Figure 3:  GFIPM Federation Phases of Membership


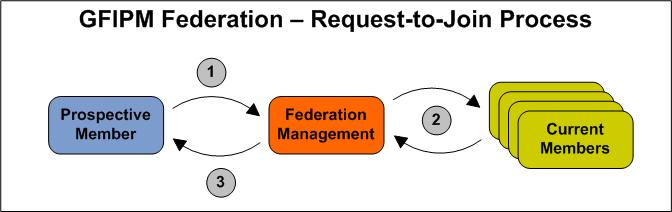

**Figure 3: GFIPM Federation Phases of Membership**

## Request-to-Join Process

The Request-to-Join Process serves as a preliminary qualifications assessment for the application process. The Request-to-Join Process works as follows:

1. The prospective member organization completes and submits a Request-to-Join Form as an Identity Provider Organization (IDPO), Service Provider Organization (SPO), or Trusted Identity Broker Organization (TIBO), as needed. Request-to-Join Form templates are available in the Appendix Section. An organization wishing to join in multiple membership roles (e.g., as both an IDPO and an SPO, or as a TIBO and an SPO) MUST submit a separate Request-to-Join Form for each membership role.
2. The Federation Management Organization (FMO) evaluates the Request-to-Join Form and decides if the perspective member has the required qualifications to submit a formal application for admission to the federation. The FMO may communicate with current federation members, at its discretion, as part of the decision-making process.
3. The FMO notifies the prospective member of the decision and invites the prospective member to submit a formal application for admission to the federation if the member’s request to join has been approved. At this time, the FMO may assign or solicit an existing member to shepherd the prospective member through the application process.

Figure 4 illustrates the Request-to-Join Process.



**Figure 4: The GFIPM Federation Request-to-Join Process**

## Application Process

The Application Process is the formal process through which a prospective member MUST be considered for admission to the federation as an IDPO, SPO, TIBO, or some combination of these. A prospective member MUST first receive approval to submit an application via the Request-to-Join Process before submitting an application for admission.

The Application Process works as follows:

1. The prospective member completes and submits to the FMO an IDPO application package, TIBO application package, or SPO application package, as required.

The IDPO application package consists of the following:

* 1. ***Completed Application Form***—a standard form on which an organization provides basic organization information about itself, e.g., name, address, names and titles of its organizational officers.
  2. ***Signed IDPO Agreement***—an agreement signed by an IDPO to indicate its intent and willingness to abide by the governance and rules of the federation
  3. ***Authority-to-Operate Document***—a document attesting to the organization’s authority to operate as an Identity Provider Organization for users under a specific legal jurisdiction
  4. ***Local Security Policy Document***—a document describing the security policy that is currently in place within the organization
  5. ***Local User Agreement Document***—a document describing the terms and conditions to which users must agree as a prerequisite for using a digital identity issued by the organization
  6. ***Local User Vetting Policies & Procedures Document***—a document describing the user vetting policies and procedures that are currently in place within the organization
  7. ***Completed IDPO Attribute Map***—a document describing how the organization plans to map its local policies and locally stored user attributes into attributes conforming to the GFIPM Metadata standard
  8. ***Completed Security Practices Checklist***[[1]](#footnote-1)—a checklist that summarizes the organization’s local security policy. The checklist is “For Information Only.” Applicants are not required to be compliant with all items on the checklist.

The SPO application package consists of the following:

1. ***Completed Application Form***—a standard form on which an organization provides basic organization information about itself, e.g., name, address, names and titles of its organizational officers.
2. ***Signed SPO Agreement***—an agreement signed by an SPO to indicate its intent and willingness to abide by the governance and rules of the federation.
3. ***Authority-to-Operate Document(s)***—a set of documents attesting to the organization’s authority to operate as a Service Provider Organization and make available electronic resources belonging to, or under the legal control of, a specific legal jurisdiction.[[2]](#footnote-2)
4. ***Local Security Policy Document***—a document describing the security policy that is currently in place within the organization.[[3]](#footnote-3)
5. ***Completed SPO Access Control Policy Map***—a document describing how the organization plans to map its local access control policies into rules that can be expressed using attributes from the GFIPM Metadata standard.
6. ***Completed Security Practices Checklist[[4]](#footnote-4)***—a checklist that summarizes the organization’s local security policy. The checklist is “For Information Only.” Applicants are not required to be compliant with all items on the checklist.

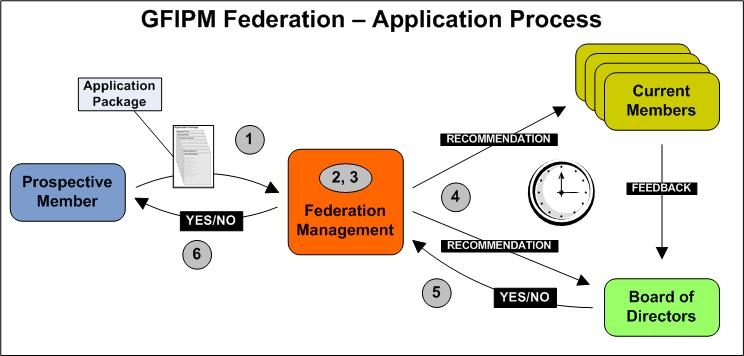
The TIBO application package consists of the following:

1. ***Completed Application Form***—a standard form on which an organization provides basic organization information about itself, e.g., name, address, names and titles of its organizational officers.
2. ***Signed TIBO Agreement***—an agreement signed by a TIBO to indicate its intent and willingness to abide by the governance and rules of the federation.
3. ***Completed Brokered IDPO Registry Form***—a document that provides the name, description, and identifier of each IDPO that the TIBO will broker.
4. ***Authority-to-Operate Document(s)***—a document or set of documents attesting to the TIBO’s authority to operate as a TIB for the users whose identities it will broker. One document is required for each IDPO (or the IDPO’s corresponding legal jurisdiction) that the TIBO will broker.
5. ***TIBO Local Security Policy Document***—a document describing the security policy currently in place within the TIBO.
6. ***Brokered IDP Local Security Policy Document(s)***—a document or set of documents describing the security policy or policies currently in place within the IDPOs that the TIBO will broker. One document is required for each brokered IDPO.
7. ***Local User Agreement Document(s)***—a document or set of documents describing the terms and conditions to which users must agree as a prerequisite for using a digital identity issued by each brokered IDPO. One document is required for each IDPO that the TIBO will broker.
8. ***Local User Vetting Policies & Procedures Document(s)***—a document or set of documents describing the user vetting policies and procedures currently in place within each brokered IDPO. One document is required for each IDPO that a TIBO will broker.
9. ***Completed Brokered Attribute Map***—a document describing how the TIBO will map the local policies and local user attributes of its brokered IDPOs into attributes conforming to [GFIPM Meta].
10. ***Completed TIBO Security Practices Checklist***—a checklist that summarizes the TIBO’s local security policy. The checklist is “For Information Only.” Applicants are not required to check “yes” for all items on the checklist as a prerequisite for membership approval.
11. ***Completed Brokered IDPO Security Practices Checklist(s)***—a checklist that summarizes the local security policy or policies of all IDPOs that the TIBO will broker. One document is required for each brokered IDPO. The checklists are “For Information Only.” Applicants are not required to check “yes” for all items on the checklist as a prerequisite for membership approval.

Template forms are located in the Appendix Section of this document. In addition, a TIBO Application Package Checklist is available to help track the collection of required documents.

1. The FMO reviews the application package for completeness and requests additional information and documents from the prospective member as needed. At this time, the FMO provides a copy of the prospective member’s IDPO Local Attribute Map (for an IDPO), SPO Local Access Policy Map (for an SPO), or Brokered Attribute Map (for a TIBO) to all current members for review and comment.
2. The FMO performs due diligence on the application package.
3. The FMO generates a recommendation to approve or deny the application and disseminates the recommendation to current federation members and the Board of Directors.[[5]](#footnote-5) To ensure that all federation members have been given adequate time to review the prospective member’s Local Attribute Map, Local Access Policy Map, or Brokered Attribute Map, the FMO shall refrain from disseminating its recommendation for at least three weeks after distributing those forms to the members.
4. If the FMO recommends approval of the prospective member’s application, then the Board of Directors and federation members must be given a three-week period to raise an objection to the approval. If no objections are raised during this period, the FMO shall grant membership to the prospective member.
   1. If an objection is raised, and the FMO agrees with the objection, the FMO may engage in a dialogue with the prospective member about what actions are necessary on the part of the prospective member to rectify the problem(s) that prevent approval of its application.
   2. If an objection is raised, and the FMO does not agree with the objection, the matter shall be handled as a dispute between a federation member and the FMO, and handled via a Board of Directors vote.
5. The FMO notifies the prospective member of the federation’s decision, and delivers a letter of membership approval to the prospective member if the application has been approved. If membership is denied, the FMO shall provide the prospective member with a set of recommendations that, if followed, would lead to subsequent approval for membership.

Figure 5 illustrates the Application Process.



**Figure 5: The GFIPM Federation Application Process**

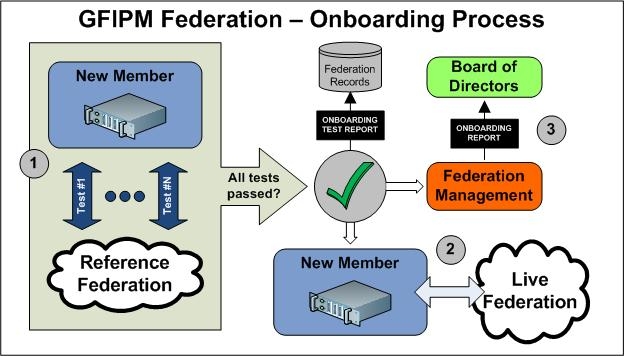
## Onboarding Process

After successfully completing the application process, the prospective member becomes an official member of the federation once all member agreements have been fully executed. At that time, the new member may begin the Onboarding Process. The Onboarding Process is a sequence of steps and tests that leads to a live, operational connection between the new member’s local information systems and the information systems of other federation members.

The Onboarding Process works as follows:

1. The new member connects its systems (IDP, SP, TIB, or any combination of these) to the GFIPM Reference Federation, and MUST pass a set of required technical interoperability tests and policy tests within the Reference Federation.[[6]](#footnote-6) After the new member has passed all of the required tests in the Reference Federation, the FMO completes an Onboarding Test Report and stores it on file. Also, after passing all required tests in the Reference Federation, the new member MUST submit a completed Implementation Documentation Form describing how its local federation-aware infrastructure is implemented.[[7]](#footnote-7) Implementation Documentation Form templates (one for an IDP and one for an SP) are available in the Appendix Section of this document.
2. After an Onboarding Test Report has been filed for the new member, the FMO adds the new member’s system(s) to the live federation’s cryptographic trust fabric. For additional information about the cryptographic trust fabric, see **[gifpm trust]**, **[gifpm cps template]**,and **[gfipm member cp template]**.
3. After the new member’s systems have been added to the live federation’s cryptographic trust fabric, the new member should be capable of interoperating with the live systems of other federation members and engaging in the information sharing process. At this time, the FMO sends an onboarding summary report to the Board of Directors.

Figure 6 illustrates the Onboarding Process.



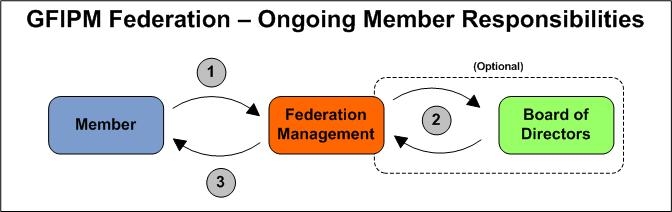
**Figure 6: The GFIPM Federation Onboarding Process**

## Ongoing Membership

After becoming a member of the federation, the new member is REQUIRED to notify the FMO of any changes to its local policies and procedures, since these may impact the member’s standing in the federation. In addition, a TIBO member organization must notify the Federation Management Organization of any changes to the local policies and procedures of any of the IDPOs that it brokers, since these may impact the TIBO’s standing in the federation and may also impact the trust relationships between the brokered IDPOs and the relying parties (SPOs) in the federation.[[8]](#footnote-8) Notification of local policy or procedural changes is subject to the following submission and approval process:

1. The member MUST provide written notification of the local change to the FMO as far in advance as possible, but no later 72 hours before the change is scheduled to take effect.
2. The FMO MAY, at its discretion, temporarily remove the member from the federation trust fabric if it is determined that the change is likely to compromise the trust relationship between the member and other federation members. In addition, the FMO MAY, at its discretion, submit the written notification to the Board of Directors and request reapproval of membership status. Board of Directors members MUST respond to the FMO within 15 days, stating whether the change is significant enough to warrant removal from the federation.
3. The FMO notifies the member of any change in its membership status, and removes the member from the federation’s cryptographic trust fabric, if necessary.

Figure 7 illustrates this process.



**Figure 7: Ongoing Member Responsibilities**

# Change Management for Normative Standards

To ensure that the federation always remains adaptable to change, the FMO shall provide a mechanism through which members and other stakeholders may propose changes to any normative standard adopted by the federation.

## Process for Proposing Changes

The FMO SHALL provide a Web site at which federation members and other stakeholders MAY submit proposals for changes to normative federation standards. In addition, the FMO SHALL publish a contact point (e.g., e-mail address) to which proposals for changes MAY be submitted. All proposals for change MUST be submitted in writing through one of these mechanisms.

## Process for Reviewing and Responding to Suggestions

The FMO SHALL respond to all proposals for changes to normative federation standards within 60 days of receiving the proposal. The FMO MAY respond to the proposal using any appropriate response mechanism at its discretion, e.g., unilateral decision, poll of federation members, or vote of Board members. When responding to the proposal for change, the FMO SHALL provide both a decision and an explanation for how it arrived at its decision.

If, after receiving the FMO’s response to the proposal for change, the submitter of the proposal believes that the FMO did not properly consider the proposal, the submitter MAY resubmit the proposal, with modifications if desired, and request that the Board of Directors cast a vote on the proposal. Any vote on a proposal by the Board of Directors SHALL be considered a final decision on the proposal.

## Submission of Vetted Changes to Global

A GFIPM Federation MUST conform to the normative standards published and defined within the Global GFIPM documentation set. It SHALL be the policy of any GFIPM Federation to submit recommended changes to technical standards to the Global Standards Council for vetting and inclusion in subsequent versions of Global GFIPM technical standards.

# Management of Federation Help Desk Services

This section describes the policies and procedures for operating a help desk for the benefit of end users. The basic purpose of a help desk is to solve operational problems raised by end users. Other related issues, such as technical assistance and onboarding assistance for member organizations, help desk staff training, and end-user training, are outside the scope of this section.

Since the federation is composed of many member organizations, each with its own local help desk resources, the federation must leverage these local resources to the maximum extent possible. The primary guiding principle in the design of the federation help desk structure is that all problems SHOULD be solved as close to the user as possible, and with as little centralized effort as possible; however, practical considerations dictate that there will be occasions when it is necessary for a central help desk entity to intervene on behalf of the FMO. Based on this principle, the following four-tier help desk structure and issue escalation plan provides guidelines for the federation.

***Tier 1: Local Help Desk Support***—All issues encountered by users SHOULD be first reported to the user’s local help desk. This level of user assistance is typically managed within the user’s local department, not at the user’s IDP. The majority of simple issues reported by users (e.g., network outages, firewall problems, and local desktop user interface issues) can and SHOULD be handled at this level without bringing any higher-level resources into play. The local help desk may track the issue in accordance with its local issue tracking policy; there is no need for such issues to be tracked at the federation level.

***Tier 2: IDP/SP Help Desk Support***—For any issue that the local help desk cannot resolve, the local help desk SHOULD refer the user to the help desk at the user’s IDP. Issues that can be solved at Tier 2 typically include questions about the use of specific services at an SP, as well as questions regarding permissions and access control policies for resources. The IDP help desk SHOULD attempt to resolve the issue, and MAY contact help desk support staff at one or more federation SPs if necessary to resolve the issue. If possible, IDP and SP help desk staff SHOULD resolve the issue without escalating it to Tier 3. Issues that are resolved at this level MAY be tracked locally by any agencies that were involved in the resolution process; however, as with Tier 1 issues, there is no need for Tier 2 issues to be tracked at the federation level.[[9]](#footnote-9)

***Tier 3: Federation Help Desk Support***—Any issue that cannot be resolved at Tier 2 SHOULD be escalated to the Federation Help Desk. Issues that can be solved at Tier 3 include repairing a corrupted version of the federation trust fabric document or resolving a technical dispute between an IDP and an SP over the question of how to solve a particular technical problem.[[10]](#footnote-10) Issues that are resolved at this level SHALL be tracked in the federation’s issue tracking database, which SHALL be available to technical staff at all IDPs and SPs in the federation.

***Tier 4: Engineering Support***—Technical issues that cannot be resolved at Tier 3 can be escalated by the Federation Help Desk to the FMO engineering support for more careful analysis. Note there may also be some business process and governance-level questions that need to be escalated from the Federation Help Desk to the FMO or the Board of Directors.

The four-tier structure described here carries certain assumptions that MUST be met for it to work effectively. These assumptions include the following.

1. All users MUST know how to contact their local help desk.
2. Help desk staff at Federation IDPs and SPs MUST have access to the necessary contact information so they can contact other IDP and SP help desks as necessary. Also, IDPs and SPs MUST make their help desk staff available to each other as needed to assist in resolving issues.
3. Help desk staff at local departments and at IDPs and SPs MUST be trained in a basic understanding of the federation concept and structure. They MUST also understand how the escalation plan works.
4. The Federation Help Desk MUST be staffed with personnel who are trained in a basic understanding of the federation concept and structure.
5. Engineering resources MUST be available to assist in resolving Tier 4 issues as needed.

# Other Considerations for Information Sharing Federations

This document aims to provide a useful guideline on some of the basic policies and procedures that are necessary for the successful operation of an information sharing federation. In particular, this document addresses those topics that have been deemed critical to the success of all such federations. While these guidelines are necessary, in most instances they are not sufficient for the operation of a federation, and therefore must be supplemented with additional policies and procedures that pertain to a specific federation’s requirements and goals. The purpose of this section is to provide a brief list of topics that a federation may wish to consider when defining a set of local policies and procedures to supplement those described in this document. The following topics are likely to be important enough to most federations to warrant inclusion in the federation’s policies and procedures document.

1. *Management of Federation Certificate Authority (CA)*—How does the federation manage its certificate authority? The GFIPM Certificate Policy Guideline **[gfipm cp]** also contains recommendations related to management of a federation CA.
2. *Management of Federation Trust Fabric*—What policies and procedures does the federation use to manage the lifecycle of its federation trust fabric? The GFIPM Cryptographic Trust Model **[gfipm ctm]** provides normative language regarding trust fabric file formats, as well as other technical details regarding the distribution of trust fabric documents; however, there are some aspects of the trust fabric management process that can be tailored to a particular federation’s needs and preferences. See **[gfipm ctm]** for more information about this topic.
3. *Management of Ancillary Federation Services*—A federation that adopts the GFIPM normative technical standards will typically need to implement one or more central federation services to address visibility of Federation Service Providers, service policies and IDP discovery for browser-based Web (portal) applications single sign-on transactions. These services are important in the day-to-day operation of an information sharing federation, but are not critical from the standpoint of interagency trust. Therefore, they are not addressed in this document.
4. *Minimum Standards for Members’ Local Business Practices*—The GFIPM Governance Guideline **[gfipm gov]** and these policies and procedures are geared toward establishing trust between federation participants based on transparency and full disclosure of local policies followed by participating agencies. But the GFIPM documents stop short of specifying any requirements regarding minimum local business practice standards that federation members must follow. Local business practice standards may include security policy standards (e.g., minimum acceptable user authentication strength, minimum time for which audit logs are kept), performance requirements (e.g., uptime, responsiveness) for services offered to the federation by members, and others as well. It is recommended that every federation carefully consider whether to impose any local business practice requirements on its members, taking into account both the benefits and the costs of such a policy.

# Glossary

**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 organizational entity that manages the day-to-day operations of the federation, including developing and maintaining standards, coordinating membership, and providing executive secretarial services to the Board of Directors.

**identity provider organization** (IDPO): A federation member organization that vets individuals, collects attributes about these individuals, and maintains these attributes in an accurate and timely manner. The IDPO operates an Identity Provider (IDP), which is a software service that performs user authentication each time an individual presents himself or herself 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 interfederation trust model between like and unlike federations.

**service provider organization** (SPO): A federation member organization that provides one or more electronic information service(s) to the federation. Service Provider Organizations provide services to the federation via Service Providers, which are trusted software services. These SPs evaluate the set of Identity Provider attributes presented to them in a form that conforms to the GFIPM Web Browser User-to-System Profile **[gfipm u2s profile]**, to determine what level of access to provide 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 attribute 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 among 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 and its users. Additionally, user obligations specified by a specific service policy is not in the scope of federation governance.

# References

FIPS 200 Federal Information Processing Standard Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

GFIPM DEMO The Georgia Tech Research Institute. GTRI Global Federation Identity and Privilege Management Security Interoperability Demonstration Report, August 30, 2007. <http://it.ojp.gov/gfipm>.

GFIPM GOV Global Standards Council. Federated Identity and Privilege Management Governance Document, Version 1.1, [Publication Date TBD].

GFIPM OPP Global Standards Council. Federated Identity and Privilege Management Operational Policies and Procedures, 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

RFC 2119 The Internet Engineering Task Force, March 1997, http://www.ietf.org/rfc/rfc2119.txt.

Appendix A—Application to Join the Federation

|  |  |  |
| --- | --- | --- |
| Name | | |
|  | (Full Legal Name of Organization) |  |
| Type of Organization | | |
|  | (Type of Organization, e.g., "Government Agency," "501(c)(3) Nonprofit Corporation," "For-Profit Corporation." Include details as needed.) |  |
| Address | | |
|  | (Physical Address of Organization) |  |
| FBI Originating Reporting Agency Identifier (ORI) Code | | |
|  | (ORI Code for Organization, if any) |  |
| Internet Web Site URL | | |
|  | (Internet Web site URL of Organization, if any) |  |
| Highest-Ranking Officer (e.g., Department Head, Agency Director, CEO) | | |
|  | (Name, Title, and Contact Information) |  |
| Second-Highest-Ranking Officer (e.g., Assistant Department Head) | | |
|  | (Name, Title, and Contact Information) |  |
| Primary Point of Contact for Application Process | | |
|  | (Name, Title, and Contact Information) |  |
| Secondary Point of Contact for Application Process | | |
|  | (Name, Title, and Contact Information) |  |
|  | | |

Appendix B—Request to Join as a Service Provider Organization

1. **Organization**

|  |  |  |
| --- | --- | --- |
| Name | | |
|  | (Name of Organization) |  |
| Description | | |
|  | (Description of Organization) |  |
|  | | |

1. **Point of Contact**

|  |  |  |
| --- | --- | --- |
| Name | | |
|  | (Name of Contact) |  |
| Title | | |
|  | (Title of Contact) |  |
| Address | | |
|  | (Address of Contact) |  |
| Phone | | |
|  | (Phone Number of Contact) |  |
|  | | |

1. **Potential Scope of Participation**

*This information helps the Federation Management Organization better understand the scope of your organization, including the number and types of services that you can provide, the legal jurisdiction(s) under which your organization operates, and any other information sharing systems or programs in which your organization currently participates.*

|  |  |  |
| --- | --- | --- |
| Summary of Available Resources | | |
|  | (List the services that the organization proposes to make available to users via the Federation. For each service, provide name, description, target user base, and legal jurisdiction granting authority to offer service data.) |  |
| Purpose for Joining the Federation | | |
|  | (Describe purpose for joining the Federation.) |  |
| Other Information Sharing Systems and Programs | | |
|  | (List and briefly describe any other information sharing systems or programs in which the organization currently participates. Also describe the scope of the organization's participation in those programs.) |  |
| Do you plan to join the Federation as an IDP also? | | |
|  | (Answer: Yes – Now, Yes – Later, or No) |  |
|  | | |

Appendix C—Request to Join as an Identity Provider Organization

1. **Organization**

|  |  |  |
| --- | --- | --- |
| Name | | |
|  | (Name of Organization) |  |
| Description | | |
|  | (Description of Organization) |  |
|  | | |

1. **Point of Contact**

|  |  |  |
| --- | --- | --- |
| Name | | |
|  | (Name of Contact) |  |
| Title | | |
|  | (Title of Contact) |  |
| Address | | |
|  | (Address of Contact) |  |
| Phone | | |
|  | (Phone Number of Contact) |  |
|  | | |

1. **Potential Scope of Participation**

*This information helps the Federation Management Organization better understand the scope of your organization, including the number and types of users that you serve, the legal jurisdiction(s) under which your organization operates, and any other information sharing systems or programs in which your organization currently participates.*

|  |  |  |
| --- | --- | --- |
| Summary of User Base | | |
|  | (Summarize the organization’s user base, e.g., “5,300 highway patrol officers,” “125 detectives.” Include both descriptions and approximate total numbers for all users who could potentially be granted permission to access Federation services.) |  |
| Legal Jurisdiction(s) | | |
|  | (Under what legal jurisdiction(s) does the organization have the authority to manage digital identities for the users listed above? Please explain.) |  |
| Purpose for Joining the Federation | | |
|  | (Describe purpose for joining the Federation.) |  |
| Other Information Sharing Systems and Programs | | |
|  | (List and briefly describe any other information sharing systems or programs in which the organization currently participates. Also describe the scope of the organization's participation in those programs.) |  |
| Do you plan to join the Federation as an SP also? | | |
|  | (Answer: Yes – Now, Yes – Later, or No) |  |
|  | | |

Appendix D—Request to Join as a Trusted Identity   
Broker Organization

1. **Organization**

|  |  |  |
| --- | --- | --- |
| Name | | |
|  | (Name of Organization) |  |
| Description | | |
|  | (Description of Organization) |  |
|  | | |

1. **Point of Contact**

|  |  |  |
| --- | --- | --- |
| Name | | |
|  | (Name of Contact) |  |
| Title | | |
|  | (Title of Contact) |  |
| Address | | |
|  | (Address of Contact) |  |
| Phone | | |
|  | (Phone Number of Contact) |  |
|  | | |

1. **Potential Scope of Participation**

*This information helps the Federation Management Organization better understand the scope of your organization, including the number and types of users that you serve, the legal jurisdiction(s) under which your organization operates, and any other information sharing systems or programs in which your organization currently participates.*

|  |  |  |
| --- | --- | --- |
| Summary of User Base | | |
|  | (Summarize the organization’s user base, e.g., “5,300 highway patrol officers,” “125 detectives.” Include both descriptions and approximate total numbers for all users who could potentially be granted permission to access Federation resources.) |  |
| Legal Jurisdiction(s) | | |
|  | (Under what legal jurisdiction(s) does the organization have the authority to manage digital identities for the users listed above? Please explain, and include information about organizations for which identities are brokered.) |  |
| Purpose for Joining the Federation | | |
|  | (Describe purpose for joining the Federation.) |  |
| Other Information-Sharing Systems and Programs | | |
|  | (List and briefly describe any other information-sharing systems or programs in which the organization currently participates. Also describe the scope of the organization's participation in those programs.) |  |
| Do you plan to join the Federation as a Service Provider Organization (SPO) also? | | |
|  | (Answer: Yes – Now, Yes – Later, or No) |  |
|  | | |

Appendix E—Implementation Documentation Form for a Service Provider

1. **SP Software Platform**

|  |  |
| --- | --- |
| **Operating System** | (SP OS Platform, e.g., "Red Hat Enterprise Linux 5," "Microsoft Windows Server 2003") |
| **Web Server** | (Web Server Platform, e.g., "Apache HTTP Server 2.2.x," "Apache Tomcat 6.x") |
| **SAML Endpoint Software** | (SAML Endpoint Software, e.g., "Shibboleth 2.1," "PingFederate 5") |
| **Other Software Details** | (Include any other details about the software implementation, e.g., proxy engine software, URL rewriting engine software.) |

1. **GFIPM Metadata Enablement of Resources**

|  |
| --- |
| (List each of the techniques used to allow your local resources to interoperate with GFIPM metadata, e.g., "group account mapping," "native enablement.") |

1. **Network Configuration Notes**

|  |
| --- |
| (Describe any unique network configuration details, e.g., transparent SSL proxying, SSL port forwarding.) |

Appendix F—Implementation Documentation Form for an   
Identity Provider

1. **IDP Software Platform**

|  |  |
| --- | --- |
| **Operating System** | (IDP OS Platform, e.g., "Red Hat Enterprise Linux 5") |
| **Web Server** | (Web Server Platform, e.g., "Apache HTTP Server 2.2.x," "Apache Tomcat 6.x") |
| **SAML Endpoint Software** | (SAML Endpoint Software, e.g., "Shibboleth 2.0," "PingFederate 5") |

1. **User Authentication Endpoint**

|  |
| --- |
| (Describe user authentication endpoint, e.g., "x.509 CCA via Tomcat.") |

1. **User Attribute Endpoint**

|  |
| --- |
| (Describe user attribute endpoint, e.g., "Windows Server 2003 Active Directory," "IBM Tivoli Directory Server.") |

1. **Network Configuration Notes**

|  |
| --- |
| (Describe any unique network configuration details, e.g., transparent SSL proxying, SSL port forwarding.) |

Appendix G—Implementation Documentation Form for a   
Trusted Identity Broker

1. **TIB Software Platform**

|  |  |
| --- | --- |
| **Operating System** | (IDP OS Platform, e.g., "Red Hat Enterprise Linux 5") |
| **Web Server** | (Web Server Platform, e.g., "Apache HTTP Server 2.2.x," "Apache Tomcat 6.x") |
| **SAML Endpoint Software** | (SAML Endpoint Software, e.g., "Shibboleth 2.0," "PingFederate 5") |

1. **User Authentication Endpoint**

|  |
| --- |
| (Describe user authentication endpoint, e.g., "x.509 CCA via Tomcat.") |

1. **User Attribute Endpoint**

|  |
| --- |
| (Describe user attribute endpoint, e.g., "Windows Server 2003 Active Directory," "IBM Tivoli Directory Server.") |

1. **Network Configuration Notes**

|  |
| --- |
| (Describe any unique network configuration details, e.g., transparent SSL proxying, SSL port forwarding.) |

Appendix H—GFIPM Member Security Practices Checklist

Please answer the following questions about the current local security policies and practices within your organization. For any response of “NO,” please include an explanation for your response in a separate document.

|  |  |  |
| --- | --- | --- |
| YES | NO | **Access Control (AC):** Does your organization limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and the types of transactions and functions that authorized users are permitted to exercise? |
| YES | NO | **Awareness and Training (AT):** Does your organization: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities? |
| YES | NO | **Audit and Accountability (AU):** Does your organization: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions? |
| YES | NO | **Certification, Accreditation, and Security Assessments (CA):** Does your organization: (i) periodically assess the security controls in organizational information systems to determine whether the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls? |
| YES | NO | **Configuration Management (CM):** Does your organization: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems? |
| YES | NO | **Contingency Planning (CP):** Does your organization establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations? |
| YES | NO | **Identification and Authentication (IA):** Does your organization identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to organizational information systems? |
| YES | NO | **Incident Response (IR):** Does your organization: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities? |
| YES | NO | **Maintenance (MA):** Does your organization: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance? |
| YES | NO | **Media Protection (MP):** Does your organization: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse? |
| YES | NO | **Physical and Environmental Protection (PE):** Does your organization: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems? |
| YES | NO | **Planning (PL):**  Does your organization develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems? |
| YES | NO | **Personnel Security (PS):** Does your organization: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures? |
| YES | NO | **Risk Assessment (RA):** Does your organization periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information? |
| YES | NO | **System and Services Acquisition (SA):**  Does your organization: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization? |
| YES | NO | **System and Communications Protection (SC):** Does your organization: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems? |
| YES | NO | **System and Information Integrity (SI):**  Does your organization: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response? |

Appendix I—Document History

| Date | Version | Editor | Change |
| --- | --- | --- | --- |
| 09/29/2008 | 0.2 | Matt Moyer,  Larry Maloney | Initial draft |
| 09/14/2010 | 1.0 | Matt Moyer | Final edits for version 1.0 |
| 05/26/2011 | 1.1 | Matt Moyer | Draft edits for version 1.1 |
| 04/12/2012 | 1.2 | Global Standards Council (GSC), Global Federated Identity and Privilege Management Delivery Team (GFIPM DT) | Approved |

BACK COVER—

About the Global Advisory Committee
www.it.ojp.gov/global
The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA’s Global Justice Information Sharing Initiative (Global). BJA engages GAC member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.  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 the Global Standards Council
www.it.ojp.gov/gsc
The Global Standards Council (GSC) serves as a Global Advisory Committee (GAC) subcommittee, supporting broadscale electronic sharing of pertinent justice- and public safety-related information by recommending to BJA (through the GAC) associated information sharing standards and guidelines. To foster community participation and reuse, the GSC reviews proposed information sharing standards submitted by Global consumers and stakeholders. Additionally, BJA emphasizes an open, participatory review-and-comment process for proposed standards; please see the Global Justice Tools Web site at www.globaljusticetools.net for more information on this opportunity. BJA-approved standards are developed, maintained, and sustained as one cohesive Global Standards Package (GSP) located 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. This checklist was derived using the FIPS 200. [↑](#footnote-ref-1)
2. One Authority-to-Operate Document is required for each jurisdiction, and each document submitted must include or be accompanied by a list of services that will be provided for the applicable jurisdiction. In addition, it is recommended that an SP submit a service level agreement (SLA) for each service that will be provided. [↑](#footnote-ref-2)
3. It is recommended that an SP submit its local user agreement and local privacy policy in addition to its local security policy document. [↑](#footnote-ref-3)
4. This checklist was derived using the FIPS 200. [↑](#footnote-ref-4)
5. If the Federation Management’s recommendation is to deny membership to the prospective member, the Federation Management may engage in a dialogue with the prospective member about what actions are necessary on the part of the prospective member to rectify the problem(s) that prevent approval of its application. [↑](#footnote-ref-5)
6. One of the goals of the Onboarding Process is to determine whether the new member is acting in accordance with its stated local policies per its application package. For example, if acting as an SP, the new member must enforce access control on its resources in accordance with the policies described in its Local Access Policy Mapping Form. If the new member is not acting in accordance with its stated intentions, and does not rectify any and all deviations from its stated policies as specified in its application package, the FMO shall have the right to invalidate the new member’s membership and force the new member to repeat the application process. [↑](#footnote-ref-6)
7. It is important for the federation to track this information, both to facilitate the onboarding process of future members and to more efficiently manage security threats and vulnerabilities. [↑](#footnote-ref-7)
8. This includes notification about the establishment of any new IDPOs that the TIBO chooses to broker to the Federation. [↑](#footnote-ref-8)
9. Note that in some cases, a Federation member organization may provide both Tier 1 and Tier 2 support using the same help desk resource. [↑](#footnote-ref-9)
10. Note that this example pertains to purely technical disputes for which the Federation Help Desk can provide an authoritative, “correct” resolution. If the nature of the dispute encompasses more than simply a technical issue, it may need to be resolved via the federation’s dispute resolution process. See [GFIPM GOV] for more information about this process. [↑](#footnote-ref-10)