National Identity Exchange Federation

Operational Policies and Procedures

Version 1.0

August 18, 2014

About this Document

The National Identity Exchange Federation (NIEF) Operational Policies and Procedures document describes the operational policies and procedures that govern the basic operation of NIEF, 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.

The target audience for this document includes managers and technical representatives of prospective NIEF Center member organizations who are planning to implement an Identity Provider (IDP), SAML Assertion Delegate Service (ADS), Service Provider (SP), Web Service Provider (WSP), Web Service Consumer (WSC), Attribute Provider (AP), or Trusted Identity Broker (TIB) role within NIEF.

Table of Contents

1. Introduction

The purpose of this document is to describe the operational policies and procedures that govern the basic operation of the National Identity Exchange Federation (NIEF), which is a trust framework for trusted identity and authentication attributes information sharing based on the Global Federated Identity and Privilege Management (GFIPM) suite of specifications and policy templates. Specifically, the policies and procedures in this document are focused on creating and maintaining a solid foundation of trust on which an information-sharing infrastructure can be built and operated.

The National Identity Exchange Federation Center (hereinafter referred to as "NIEF Center") at the Georgia Institute of Technology (GIT) has been established to:

- Advance and support programs that facilitate the sharing of justice and public safety information among Federal, state, local, and tribal justice and public safety agencies in a timely and cost efficient manner;

- Enable, operate, maintain, enhance, and expand the secure, standards based, inter- and intra-state sharing of information through the Global Federated Identity and Privilege Management (GFIPM) concept;

- Provide education concerning the associated standards and concepts of operation; and

- Establish, operate, govern, and maintain the National Identity Exchange Federation (NIEF) and perform the role and all of the associated duties and responsibilities of the Federation Manager on behalf of the members of the NIEF Center.

Information sharing with and among state, local, tribal, and federal agencies will be stimulated by Membership in the NIEF Center and participation in NIEF.

The NIEF Center is established by the Georgia Tech Applied Research Corporation ("GTARC"), a tax-exempt entity under Section 501(c)(3) of the Internal Revenue Code of 1986, as amended (Code) and a supporting organization of the Georgia Institute of Technology ("GIT") under Section 509(a)(3) of the Code. Figure 1 depicts the organizational governance structure for the NIEF Center.

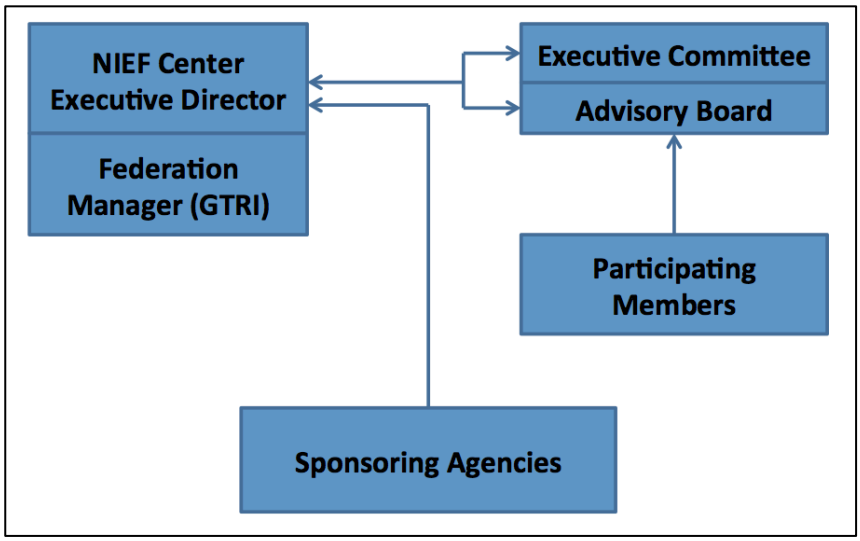

Figure 1: Organizational Governance Structure for the NIEF Center

The NIEF Center Executive Director shall lead the NIEF Center with the assistance of the Members through an Advisory Board (AB) whose purpose it will be to advise the Director on the direction of activities and the operational policies of the Center and the Federation. The AB, facilitated by the Director, shall work collaboratively to arrive at consensus recommendations for the benefit of the Federation. The Director of the NIEF Center shall make final decisions on behalf of the NIEF Center and be responsible for the general management of the day-to-day affairs of the NIEF Center. The Federation Management Organization (FMO) is the organizational entity at Georgia Tech, under the direction of the NIEF Center Director, which manages the day-to-day operations of NIEF Center, including developing and maintaining standards, coordinating membership, and providing executive secretarial services to the Advisory Board.

The membership of the NIEF Center shall consist of federal, state, local and tribal justice and public safety agencies and other duly recognized non-profit organizations supporting justice and public safety in the United States that have signed agreements with GTARC acting on behalf of the NIEF Center at GIT. Members must successfully complete the on-boarding process as Identity Provider Organizations (IDPOs), Service Provider Organizations (SPOs), Attribute Provider Organizations (APOs), Service Consumer Organizations (SCOs), Trusted Identity Broker Organizations (TIBOs), or other stakeholder members as may be determined by the Director, in accordance with the governance policy and procedures contained herein and with the advice of the Executive Committee (EC) as defined in this document. Organizations which on-board in more than one role (IDPO, SPO, APO, SCO, or TIBO) would be considered a single Member of the NIEF Center and provide a single representative with a single vote on the AB.

A majority vote of the Member representatives to the AB shall elect an Executive Committee (EC) of no more than seven members who provide representation of IDPOs, SPOs, APOs, SCOs, TIBOs, and Stakeholder agencies. The EC will elect from among its

members a Chair to lead the AB and the EC, and a Vice-Chair to act in his/her stead in the event that the Chair is not available.

The EC will (a) advise the NIEF Center Director on any modification necessary to standard Participation Agreements, (b) advise the NIEF Center Director of any needed changes in other Federation governance documents or the structure of governance, and (c) act on behalf of the AB between meetings of the AB. The NIEF Center Bylaws further define roles and responsibilities of the EC, AB, and NIEF Center Director.

Figure 2 defines the two fundamental policy layers that facilitate secure information sharing within a GFIPM-based federation or trust framework.

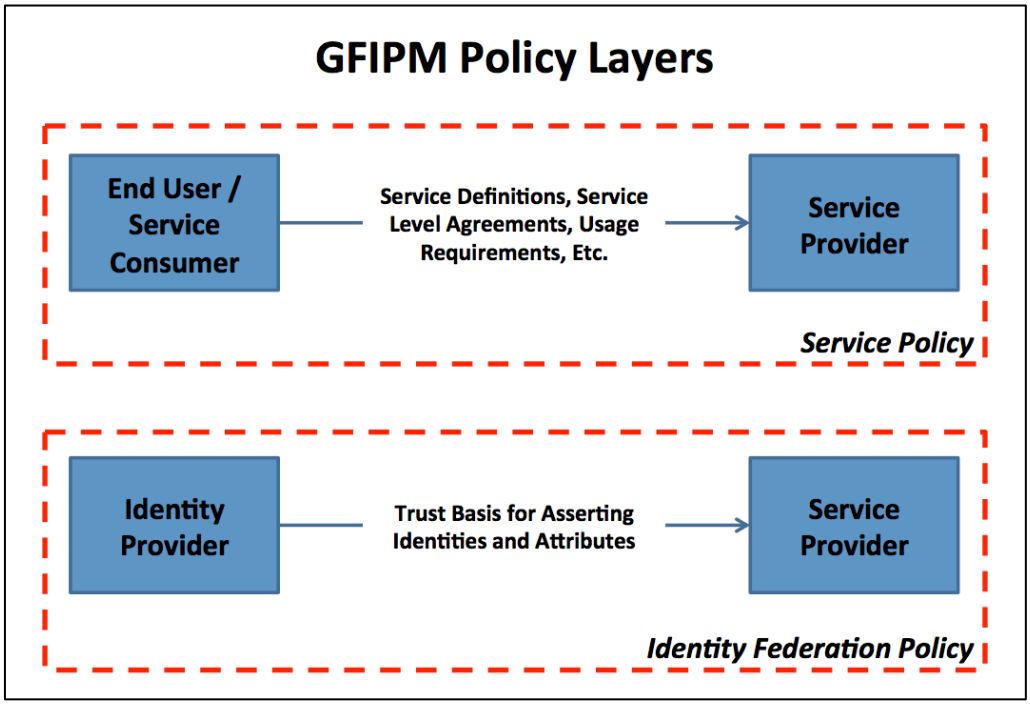

Figure 2: Policy Layers in a GFIPM Federation or Trust Framework

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 between NIEF members at the identity federation policy layer. Some members may have additional service level policy requirements, which need to be layered on top of the base NIEF agreements and policies. While complementary with the NIEF governance and approach, those policies, processes, and procedures are considered outside the scope of this document.

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

2. Federation Document Structure

Figure 3 illustrates the complete set of NIEF federation documents relating to governance, operations, and technical standards.

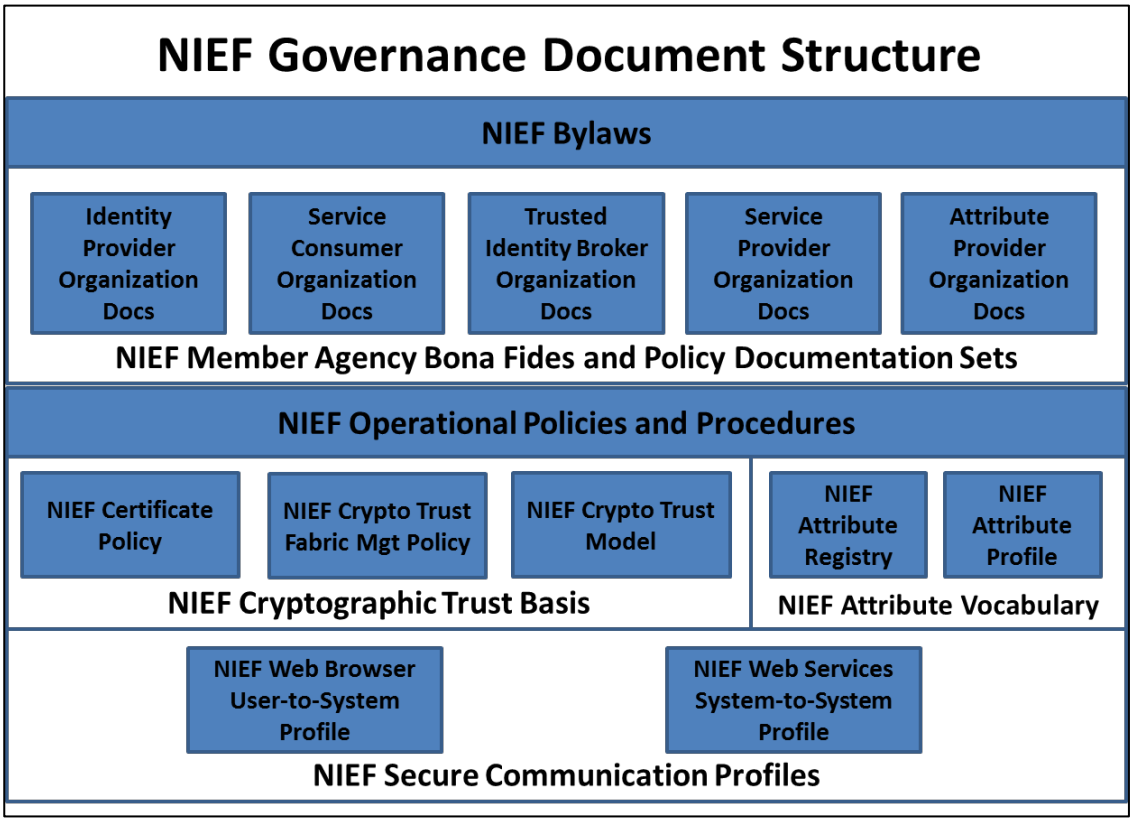

Figure 3: NIEF Governance Document Structure

As illustrated in Figure 3, the NIEF federation governance and technical document structure consists of the following documents.

- **NIEF Bylaws [NIEF Bylaws]**—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.

- **NIEF Member Agency Bona Fides and Policy Documentation Sets**—Documents provided by participating member agencies in accordance with NIEF requirements as specified within Section 6 of [NIEF OPP].

- **NIEF Operational Policies and Procedures [NIEF OPP]**—Details the way in which the federation policies will be carried out.

- **NIEF Cryptographic Trust Model [NIEF Trust]**—Details the technical requirements for maintaining cryptographic trust among systems in the Federation.

- **NIEF Certificate Policy [NIEF CP]**—Details the certificate and key management policy that all Federation participants must follow to ensure cryptographic trust is maintained among systems in the Federation.

- **NIEF Cryptographic Trust Fabric Management Policy [NIEF CTFMP]**-Details the procedures to be used by the NIEF Center and its participants for the assembly, maintenance, and distribution of the NIEF Cryptographic Trust Fabric document.

- **NIEF Attribute Registry [NIEF Attrs]**—Contains a set of attributes that may be used within NIEF.

- **NIEF Attribute Profile [NIEF AP]**—Contains requirements on NIEF IDPOs related to attributes that appear in the NIEF Attribute Registry.

- **NIEF Attribute Encoding Rules [NIEF Attr Enc]**—(Not Shown in Diagram) Contains requirements related to encoding of attributes within various structures, including SAML assertions and NIEF Cryptographic Trust Fabric.

- **NIEF Web Browser User-to-System Profile [NIEF U2S Profile]** and **NIEF Web Services System-to-System Profile [NIEF S2S Profile]**—Detail the technical interfaces required to implement specific communication profiles in the Federation.

3. 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 inter-organizational identity and access control trust model.

4. Compliance with Federation Policies and Procedures

4.1 Definitive Authority and Scope of NIEF Identity Trust Framework

This document is the definitive authority on all NIEF Operational Policies and Procedures. It incorporates by reference the following other documents. Together, these documents constitute the full NIEF Identity Trust Framework.

Document ID	Document Name
[NIEF Terms]	NIEF Terminology Reference
[NIEF Bylaws]	NIEF Bylaws
[NIEF Trust]	NIEF Cryptographic Trust Model
[NIEF CP]	NIEF Certificate Policy
[NIEF CTFMP]	NIEF Cryptographic Trust Fabric Management Policy
[NIEF Privacy]	NIEF Privacy Policy
[NIEF Audit]	NIEF Audit Policy
[NIEF Attrs]	NIEF Attribute Registry
[NIEF AP]	NIEF Attribute Profile
[NIEF Attr Enc]	NIEF Attribute Encoding Rules
[NIEF U2S Profile]	NIEF Web Browser User-to-System Profile
[NIEF S2S Profile]	NIEF Web Services System-to-System Profile

Table 1: Document References for Components of the NIEF Framework

4.2 NIEF Policy on Changes to the NIEF Identity Trust Framework

Over time, the documents that comprise the NIEF Identity Trust Framework may undergo various changes to meet the evolving needs of the NIEF Center and the community that it serves. Upon approval of changes to any document or documents in the NIEF Identity Trust Framework, all current members of NIEF shall be immediately and automatically bound to the updated Framework. Any exceptions to this policy shall be agreed upon in writing between the NIEF Center and the affected member or members.

4.3 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 NIEF participants, including members and the NIEF Federation Management Organization (FMO), must comply with the normative portions of this document.

5. Types of NIEF Membership

NIEF currently offers the following types of membership.

1. **FICAM LOA 3 Identity Provider Organization (IDPO)** – This type of membership enables the member to make assertions to U.S. Federal Government agencies on behalf of its End-Users at Level of Assurance (LOA) 3 under the Federal Credentialing, Identity, and Access Management (FICAM) program. It also enables the member to make assertions on behalf of its End-Users to all NIEF SPOs, thereby enabling the member's End-Users to access NIEF SPO resources in accordance with the SPOs' access policies. Attaining and maintaining this type of NIEF membership requires that an agency complete the full IDPO onboarding process as defined in Section 6 of this document. Note that this includes initial and ongoing audits at LOA 3 in accordance with [NIEF Audit]. Note also that all assertions made about End-Users are subject to NIEF privacy rules as specified in [NIEF Privacy].

2. **FICAM LOA 2 Identity Provider Organization (IDPO)** – This type of membership enables the member to make assertions to U.S. Federal Government agencies on behalf of its End-Users at LOA 2 under the FICAM program. It also enables the member to make assertions on behalf of its End-Users to all NIEF SPOs, thereby enabling the member's End-Users to access NIEF SPO resources in accordance with the SPOs' access policies. Attaining and maintaining this type of NIEF membership requires that an agency complete the full IDPO onboarding process as defined in Section 6 of this document. Note that this includes initial and ongoing audits at LOA 2 in accordance with [NIEF Audit]. Note also that all assertions made about End-Users are subject to NIEF privacy rules as specified in [NIEF Privacy].

3. **Non-FICAM Identity Provider Organization (IDPO)** – This type of membership enables the member to make assertions on behalf of its End-Users to all NIEF SPOs, thereby enabling the member's End-Users to access NIEF SPO resources in accordance with the SPOs' access policies. Attaining and maintaining this type of NIEF membership requires that an agency complete the full IDPO onboarding process as defined in Section 6 of this document. Note that all assertions made about End-Users are subject to NIEF privacy rules as specified in [NIEF Privacy].

4. **Service Provider Organization** – This type of membership enables the member to serve digital resources and services to other NIEF member agencies and their End-Users, in accordance with the member's local access policy. Attaining and maintaining this type of NIEF membership requires that an agency complete the full SPO onboarding process as defined in Section 6 of this document.

5. **Service Consumer Organization** – This type of membership enables the member to consume digital resources and services from other NIEF SPOs in accordance with the SPOs' local access policies. Attaining and maintaining this type of NIEF membership requires that an agency complete the full SCO onboarding process as defined in Section 6 of this document.

6. **Attribute Provider Organization** – This type of membership enables the member to assert attributes to other NIEF member organizations on behalf of End-Users for whom the member maintains attribute data. Attaining and maintaining this type of

NIEF membership requires that an agency complete the full APO onboarding process as defined in Section 6 of this document. Note that all assertions made about End-Users are subject to NIEF privacy rules as specified in [NIEF Privacy].

7. **Trusted Identity Broker Organization** – This type of membership enables the member to broker assertions to all NIEF SPOs on behalf of End-Users from IDPs that do not belong to NIEF IDPOs, thereby enabling the End-Users to access NIEF SPO resources in accordance with the SPOs' access policies. Attaining and maintaining this type of NIEF membership requires that an agency complete the full TIBO onboarding process as defined in Section 6 of this document. Note that all assertions made about End-Users are subject to NIEF privacy rules as specified in [NIEF Privacy].

In general, an organization may apply for any of the available membership types, and may hold multiple membership types simultaneously; however, an organization can hold only one type of IDPO membership at a time.

6. 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 4 illustrates this sequence of phases, and sections 6.1 through 6.4 define each phase and its associated process and requirements.

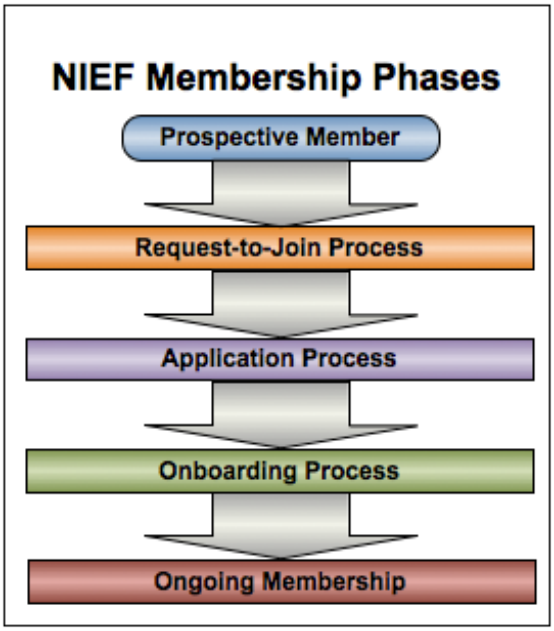

Figure 4: NIEF Membership Phases

6.1 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), Attribute Provider Organization (APO), Service Consumer Organization (SCO), or Trusted Identity Broker Organization (TIBO), as needed. Request-to-Join Form templates are available at https://nief.gfipm.net/prospective/. 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. Note that an organization may not join as both an IDPO and an APO[1].

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.

[1] The requirements for IDPOs subsume the requirements for APOs. If an organization wishes to provide attributes that constitute Personally Identifiable Information (PII) to federation members on behalf of its users, then that organization must join as an IDPO. If an organization wishes to provide only non-PII user attributes about users, then that organization may join as an APO.

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 5 illustrates the Request-to-Join Process.

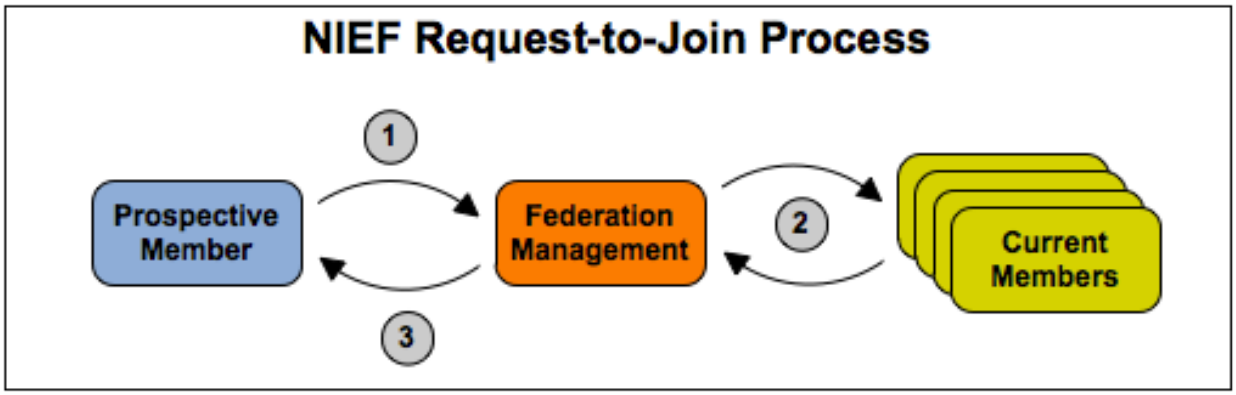

Figure 5: The NIEF Request-to-Join Process

6.2 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, APO, SCO, 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, APO application package, TIBO application package, SCO application package, or SPO application package, as required.

   The IDPO application package consists of the following contents.

   a. ***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. An Application Form template is available for download at the Application Forms and Templates page of the NIEF website.[2]

[2] https://nief.gfipm.net/prospective/application-forms-and-templates/

b. ***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. An IDPO Agreement template is available for download at the Application Forms and Templates page of the NIEF website.

c. ***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.

d. ***Local Security Policy Document***—a document describing the security policy that is currently in place within the organization.

e. ***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.

f. ***Local User Vetting Policies & Procedures Document***—a document describing the user vetting policies and procedures that are currently in place within the organization.

g. ***Completed IDPO Attribute Map***—a document describing how the organization plans to map its local policies and locally stored user attributes into attributes from [NIEF Attrs]. An IDPO Attribute Map template is available for download at the Application Forms and Templates page of the NIEF website.

h. ***Completed Security Practices Checklist***[3]—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. A Security Practices Checklist Form template is available for download at the Application Forms and Templates page of the NIEF website.

The SPO application package consists of the following contents.

a. ***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. An Application Form template is available for download at the Application Forms and Templates page of the NIEF website.

b. ***Signed SPO Agreement***—an agreement signed by an SPO to indicate its intent and willingness to abide by the governance and rules of the

[3] This checklist was developed using [FIPS 200].

federation. An SPO Agreement template is available for download at the Application Forms and Templates page of the NIEF website.

c. ***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.[4]

d. ***Local Security Policy Document***—a document describing the security policy that is currently in place within the organization.[5]

e. ***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 [NIEF Attrs]. An SPO Access Control Policy Map template is available for download at the Application Forms and Templates page of the NIEF website.

f. ***Completed Security Practices Checklist[6]***—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. A Security Practices Checklist template is available for download at the Application Forms and Templates page of the NIEF website.

The APO application package consists of the following contents.

a. ***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. An Application Form template is available for download at the Application Forms and Templates page of the NIEF website.

b. ***Signed APO Agreement***—an agreement signed by an APO to indicate its intent and willingness to abide by the governance and rules of the federation. An APO Agreement template is available for download at the Application Forms and Templates page of the NIEF website.

[4] 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.

[5] It is recommended that an SP submit its local user agreement and local privacy policy in addition to its local security policy document.

[6] This checklist was developed using [FIPS 200].

c. ***Authority-to-Operate Document***—a document attesting to the organization's authority to operate as an Attribute Provider Organization for a specific set of attributes and users.

d. ***Local Security Policy Document***—a document describing the security policy that is currently in place within the organization.

e. ***Completed APO Attribute Map***—a document describing how the organization plans to map its local policies and locally stored user attributes into attributes from [NIEF Attrs]. An APO Attribute Map template is available for download at the Application Forms and Templates page of the NIEF website.

f. ***Completed Security Practices Checklist***[7]—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. A Security Practices Checklist template is available for download at the Application Forms and Templates page of the NIEF website.

The SCO application package consists of the following contents.

a. ***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. An Application Form template is available for download at the Application Forms and Templates page of the NIEF website.

b. ***Signed SCO Agreement***—an agreement signed by an SCO to indicate its intent and willingness to abide by the governance and rules of the federation. An SCO Agreement template is available for download at the Application Forms and Templates page of the NIEF website.

c. ***Authority-to-Operate Document(s)***—a set of documents attesting to the organization's authority to operate as a Service Consumer Organization.

d. ***Local Security Policy Document***—a document describing the security policy that is currently in place within the organization.

e. ***Completed Security Practices Checklist***[8]—a checklist that summarizes the organization's local security policy. The checklist is "For Information Only." Applicants are not required to be compliant

[7] This checklist was developed using [FIPS 200].
[8] This checklist was developed using [FIPS 200].

with all items on the checklist. A Security Practices Checklist template is available for download at the Application Forms and Templates page of the NIEF website.

The TIBO application package consists of the following contents.

a. ***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. An Application Form template is available for download at the Application Forms and Templates page of the NIEF website.

b. ***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. A TIBO Agreement template is available for download at the Application Forms and Templates page of the NIEF website.

c. ***Completed Brokered IDPO Registry Form***—a document that provides the name, description, and identifier of each IDPO that the TIBO will broker. A Brokered IDPO Registry Form template is available for download at the Application Forms and Templates page of the NIEF website.

d. ***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.

e. ***TIBO Local Security Policy Document***—a document describing the security policy currently in place within the TIBO.

f. ***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.

g. ***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.

h. ***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.

i. ***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 from [NIEF Attrs]. A Brokered Attribute Map template is available for download at the Application Forms and Templates page of the NIEF website.

j. ***Completed TIBO Security Practices Checklist***[9]—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. A Security Practices Checklist template is available for download at the Application Forms and Templates page of the NIEF website.

k. ***Completed Brokered IDPO Security Practices Checklist(s)***[10]—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. A Security Practices Checklist template is available for download at the Application Forms and Templates page of the NIEF website.

To help track the collection of required documents during the TIBO application process, a TIBO Application Package Checklist is available for download at the Application Forms and Templates page of the NIEF website.

2. 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 Attribute Map (for an IDPO), SPO Local Access Policy Map (for an SPO), APO Attribute Map (for an APO), or Brokered Attribute Map (for a TIBO) to all current NIEF members for review and comment.

3. The FMO performs due diligence on the application package.

4. The FMO conducts an initial audit of the applicant, in accordance with the NIEF Audit Policy ([NIEF Audit]) based on the types of NIEF membership sought by the applicant. See Section 5 of this document for more

[9] This checklist was developed using [FIPS 200].
[10] This checklist was developed using [FIPS 200].

information about the various types of NIEF membership that are available.

5. The FMO generates a recommendation to approve or deny the application and disseminates the recommendation to the AB.[11] 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.

6. If the FMO recommends approval of the prospective member's application, then the AB 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 after ratification by the EC.

    a. 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.

    b. 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 an AB vote with ratification by the EC.

7. 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 6 illustrates the Application Process.

[11] 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.

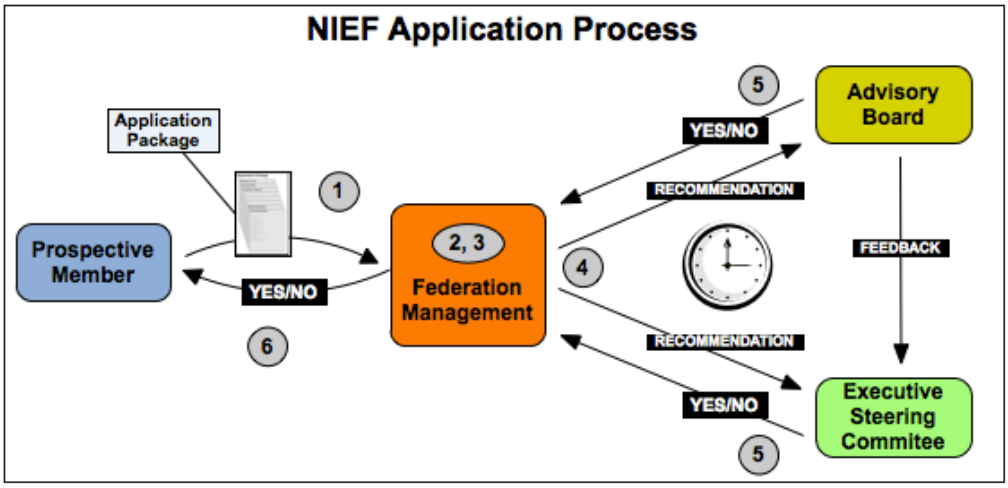

Figure 6: The NIEF Application Process

6.3 Onboarding Process

After successfully completing the application process, the prospective member becomes an official member of the NIEF Center and 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 to the GFIPM Reference Federation, and MUST pass a set of required technical interoperability tests and policy tests within the Reference Federation.[12] 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.[13] Implementation Documentation Form templates are available for download at the Application Forms and Templates page of the NIEF website.

[12] 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 Map. 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.

[13] 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.

2. After an Onboarding Test Report has been filed for the new member, the FMO adds the new member's system(s) to the NIEF cryptographic trust fabric. For additional information about the cryptographic trust fabric, see [NIEF Trust] and [NIEF CP].

3. After the new member's systems have been added to the NIEF 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 may send an onboarding summary report to the AB and EC.

Figure 7 illustrates the Onboarding Process.

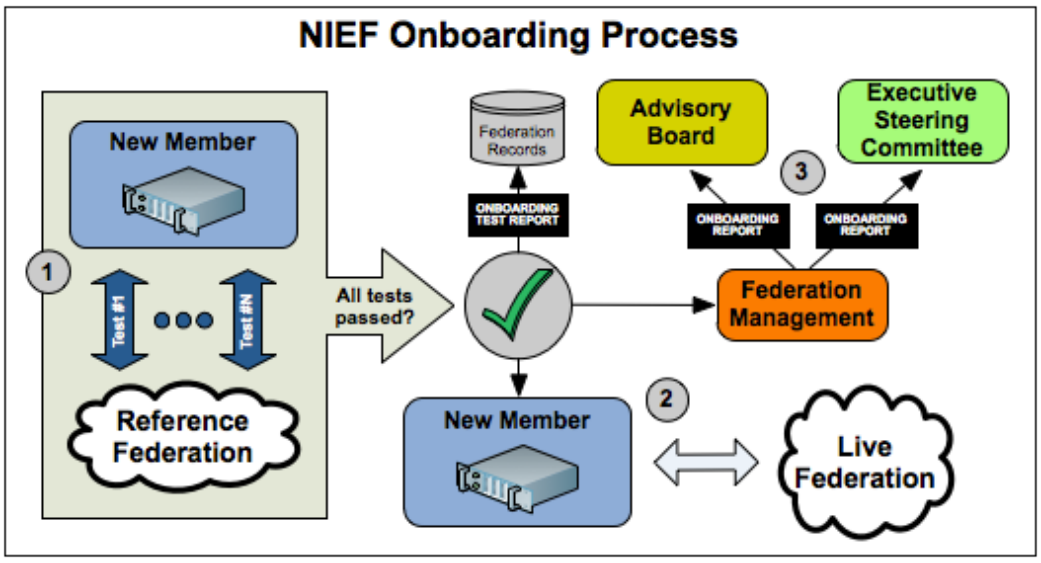

Figure 7: The NIEF Onboarding Process

6.4 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, as 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, as 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.[14] Notification of local policy or procedural changes is subject to the following submission and approval process:

[14] This includes notification about the establishment of any new IDPOs that the TIBO chooses to broker to the Federation.

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 AB and request reapproval of membership status. AB 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 8 illustrates this process.

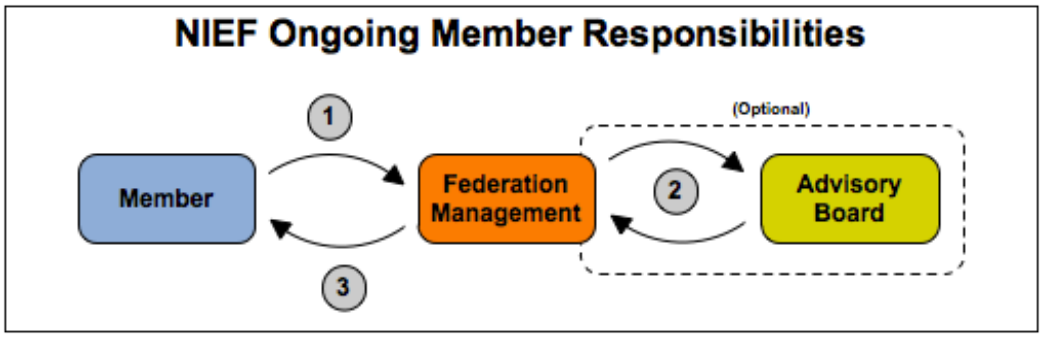

Figure 8: Ongoing NIEF Member Responsibilities

7. Initial and Ongoing Audit Process for Member Agencies

To increase the level of assurance and trustworthiness in NIEF and its member agencies, the FMO shall conduct initial and ongoing audits of all member agencies, in accordance with the process specified in [NIEF Audit].

8. 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.

8.1 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.

8.2 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 AB or EC. 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 re-submit the proposal, with modifications if desired, and request that the AB and EC be polled for their votes on the proposal. The NIEF Center Director SHALL render a final decision and explanation with due consideration of the inputs received from the AB and EC.

8.3 Submission of Vetted Changes to Global

It SHALL be the policy of NIEF to submit recommended changes to technical standards to the Global Standards Council, or other Global committee(s) as appropriate, for vetting and inclusion in subsequent versions of Global GFIPM technical standards as appropriate based on the needs of the NIEF community.

9. Management of Federation Help Desk Services

This section describes the recommended 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.

As the federation is comprised 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 members if necessary to resolve the issue. If possible, 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.[15]

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 or resolving a technical dispute between an IDP and an SP over the question of how to solve a particular technical problem.[16] Issues that are resolved at this level SHALL be tracked in the federation's issue tracking database, which SHALL be available to technical staff from all federation members.

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 AB.

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 member organizations MUST have access to the necessary contact information so they can contact other federation

[15] Note that in some cases, a Federation member organization may provide both Tier 1 and Tier 2 support using the same help desk resource.

[16] 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.

member help desks as necessary. Also, federation members MUST make their help desk staff available to each other as needed to assist in resolving issues.

3. All help desk staff at federation member organizations 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.

10. Glossary

ADVISORY BOARD (AB): Consists of representatives of the membership of the NIEF Center that have successfully completed the on-boarding process as Identity Provider Organizations (IDPOs), Service Provider Organizations (SPOs), Attribute Provider Organizations (APOs), Trusted Identity Broker Organizations (TIBOs), or other stakeholder members as may be determined by the Director, in accordance with federation governance policy and procedures and with the advice of the Executive Committee as defined below. Organizations which on-board in more than one role (IDPO, SPO, or TIBO) would be considered a single Member of the NIEF Center and provide a single representative with a single vote on the AB.

ATTRIBUTE PROVIDER ORGANIZATION (APO): An identity federation member organization that vets and collects specific attributes about individuals, maintains those attributes in an accurate manner, and provides those attributes to other organizations in the identity federation as needed, subject to applicable privacy policy, for access control and auditing purposes. An APO operates an Attribute Provider (AP), which is a software service that resolves queries for user attributes.

EXECUTIVE COMMITTEE (EC): This is the executive level body elected from the membership of the AB that will: a) advise the NIEF Center Director on any modification necessary to standard Participation Agreements, b) advise the NIEF Center Director of any needed changes in other Federation governance documents or the structure of governance, and c) act on behalf of the AB between meetings of the AB.

FEDERATION MANAGEMENT ORGANIZATION (FMO): This is the organizational entity at Georgia Tech, under the direction of the NIEF Center Director, that manages the day-to-day operations of NIEF Center, including developing and maintaining standards, coordinating membership, and providing executive secretarial services to the Advisory Board.

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 may operate 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. The IDPO may also operate an Attribute Provider (AP), which is a software service that resolves queries for user attributes.

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

SERVICE CONSUMER ORGANIZATION (SCO): A federation member organization that accesses and consumes data from one or more electronic information services in the federation for business purposes. Service Consumer Organizations provide services to the federation via Web Service Consumers, which are trusted software endpoints that communicate with Web Service Providers (WSPs).

SERVICE PROVIDER ORGANIZATION (SPO): A federation member organization that provides one or more electronic information services 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 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.

11. References

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

NIEF Bylaws	National Identity Exchange Federation Bylaws
NIEF OPP	National Identity Exchange Federation Operational Policies and Procedures
NIEF Privacy	National Identity Exchange Federation Privacy Policy
NIEF Audit	National Identity Exchange Federation Audit Policy
NIEF Trust	National Identity Exchange Federation Cryptographic Trust Model
NIEF CP	National Identity Exchange Federation Certificate Policy
NIEF CTFMP	National Identity Exchange Federation Cryptographic Trust Fabric Management Policy
NIEF Attrs	National Identity Exchange Federation Attribute Registry https://nief.gfipm.net/attribute-registry/
NIEF AP	National Identity Exchange Federation Attribute Profile
NIEF Attr Enc	National Identity Exchange Federation Attribute Encoding Rules
NIEF U2S Profile	National Identity Exchange Federation Web Browser User-to-System Profile
NIEF S2S Profile	National Identity Exchange Federation Web Services System-to-System Profile
RFC 2119	The Internet Engineering Task Force, March 1997 http://www.ietf.org/rfc/rfc2119.txt

12. Document History

Date	Version	Editors	Change
Mar 27, 2011	N/A	Matt Moyer, John Wandelt	Initial Draft
Jan 16, 2013	N/A	Matt Moyer	Added new material related to web services.
Feb 26, 2013	N/A	Matt Moyer	Added references to new NIEF policy docs for FICAM alignment.
Mar 15, 2013	N/A	Matt Moyer	Changed name of NIEF to "National Identity Exchange Federation".
Sep 27, 2013, Mar 18, 2014	N/A	E. Anwar Reddick, Matt Moyer	Added new material related to Attribute Providers.
Apr 15, 2014, Aug 18, 2014	1.0	Matt Moyer, E. Anwar Reddick	Updated diagrams and other material as needed for FICAM alignment, etc.

Editors

Matt Moyer	John Wandelt	E. Anwar Reddick