United States
Department of Justice

U.S. Department of Justice's Global

Federated Identity and Privilege Management (GFIPM)

Metadata Specification 2.0 Overview and Usage

Version 1.0

Global Security Working Group

May 2011

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

Table of Contents

Acknowledgements

The Global Federated Identity and Privilege Management (GFIPM) initiative is supported through joint funding of the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ), Office of Justice Programs, with collaboration from the Bureau of Justice Assistance and the National Institute of Justice.

The Global Justice Information Sharing Initiative (Global) aids its member organizations and the people they serve through a number of important initiatives. The Global Security Working Group (GSWG) is one of four Global Working Groups covering critical topics such as intelligence, privacy, security, outreach, and standards. The GSWG provides oversight for GFIPM with the objective of recommending a standards-based justice credential. The GSWG and the GFIPM Project are under the direction of Mr. John Ruegg, Los Angeles County Information Systems Advisory Body (ISAB). Special recognition goes to Mr. Ruegg for his strong leadership and to the volunteer-based membership of the GSWG, including the GFIPM Delivery Team and the Technical Privacy Task Team, whose members are dedicated to providing their time and expertise to ensure secure and trusted information sharing among justice organizations.

To develop this GFIPM Metadata Specification, Global has relied on the advice, expertise, knowledge, and contribution of many collaborators, justice practitioners, and industry members. Primary contributors were security experts from DHS, DOJ, Global, and Georgia Tech Research Institute (GTRI). Sincere appreciation is expressed to Mr. John Wandelt and the GFIPM Project team at GTRI for their guidance, operational management, and deep subject expertise. In addition, components of this specification were based on the partnership and early work efforts of Pennsylvania JNET, RISSNET, and CISAnet. Without these strong partnerships, this work effort would not have been possible.

For more information about Global efforts, including the GFIPM initiative and corresponding deliverables, please refer to the Global Web site at http://it.ojp.gov/GFIPM for official announcements.

1. Introduction

The concept of common, or globally understood, metadata across a federation of systems is the critical success factor for Global Federated Identity and Privilege Management (GFIPM) interoperability. A standard set of security attributes about users' identities, privileges, and authentication details can be universally communicated among partners within an information sharing environment and can help form a basis for interagency trust. This common metadata, in the form of an *assertion* between systems, allows data owners (service providers) to make independent data access and data privacy enforcement decisions based on their trust in the security assertions about users who are requesting access to specific data or data system resources.

The GFIPM Metadata 2.0 specification defines common syntax and semantics for metadata describing *users*, *entities* (trusted software service endpoints), *resources* (sensitive data objects, databases, documents, etc.), *actions* (attempts by users or entities to access resources), and the data-sharing *environment* in which actions occur. This metadata can be used in support of identification, authentication, privilege management, auditing, and personalization across a federation.

The GFIPM metadata has been developed based on data requirements and feedback from GFIPM Delivery Team members, Global Security Working Group (GSWG) members, and other GFIPM stakeholders. The current version is expected to expand and mature over time as content is refined and additional metadata requirements are gathered from the Global community, partners, and additional GFIPM project participants.

2. Scope of GFIPM Metadata Specification

The GFIPM Metadata Specification can include any attribute that represents a concept meeting the following criteria:

1. Two or more agencies can agree on the attribute's *applicability* to identity and privilege management for the purpose of secure interagency information sharing.

2. Two or more agencies can agree on a *common definition* and content for the attribute.

3. The attribute is *semantically distinct* from existing GFPIM attributes.

Version 2.0 of the specification represents a significant expansion of the scope of the GFIPM Metadata Specification. Previous versions of the specification defined attributes pertaining to users and entities. But version 2.0 includes three new categories of attributes; in addition to user attributes and entity attributes, it also contains resource attributes, action attributes, and

environment attributes. This expansion serves to encompass the full range of metadata that can pertain to an information sharing transaction and the access control policies to which a transaction must conform. The five categories of metadata attributes correspond loosely to the types of metadata that are supported within the Extensible Access Control Markup Language (XACML). The remainder of this section provides a definition for each metadata attribute category.

Entity Attributes

An entity attribute pertains to a trusted service endpoint in the federation. It can be vetted and asserted by a federation manager. Also, any changes to its value are independent of transactional context, i.e., its value tends to remain constant across transactions. Examples of entity attributes include "Entity ID," "Owner Agency Name," and "Owner Agency ORI."

User Attributes

A user attribute pertains to a human user. It can be vetted and asserted by an identity provider. Also, any changes to its value are independent of transactional context, i.e., its value tends to remain constant across transactions. Examples of user attributes include "Federation ID," "First Name," "Last Name," and "Sworn Law Enforcement Officer Indicator."

Resource Attributes

A resource attribute pertains to an access-controlled data resource secured by a service provider. It is typically determined by policy and assigned by resource owner or service provider. Examples of resource attributes include "Criminal History Data Indicator" and "Criminal Intelligence Data Indicator."

Action Attributes

An action attribute pertains to the transactional context in which a user attempts to access a resource. It is generally asserted by the user or inferred by the application through which the user initiates the action. It can contain any information about a user or entity, but only if the information pertains to a specific action and not all actions taken by the user or entity. Examples of action attributes include "Authorized Purpose" (the business purpose for which the user is taking an action) and "Geolocation" (the latitude/longitude from which an action was taken).

Environment Attributes

An environment attribute pertains to the prevailing environmental conditions in which an information sharing transaction occurs. The service provider determines its value at the time an information sharing transaction occurs. It can contain any information about an

information sharing transaction that does not pertain specifically to the transaction's entity, user, resource, or action. Examples of environment attributes include "Homeland Security Threat Level," "Time of Day," and "Weather Advisories."

3. Metadata Package Contents

The GFIPM Metadata 2.0 Specification consists of the following artifacts.

Artifact Name	Description/Purpose
Overview and Usage Document (this document)	Provides background and overview information about the metadata package, as well as miscellaneous details about usage of the metadata specification.
GFIPM Metadata 2.0 HTML Representation	Provides a browsable Hypertext Markup Language (HTML) version of the contents of the metadata specification. Posted online at http://gfipm.net/standards/metadata/2.0/.
GFIPM Metadata 2.0 PDF Representation	Provides a printable Portable Document Format (PDF) version of the contents of the metadata specification.
GFIPM Metadata 2.0 Excel Representation	Provides a Microsoft Excel version of the contents of the metadata specification.
GFIPM Metadata 2.0 Sample Profile	Provides an example of how to define a *federation profile*, which is a formal description of the subset of GFIPM Metadata attributes used within a federation, and typically specifies details such as mandatory attributes versus optional attributes, etc.
Sample SAML 2.0 Assertions	Provides examples of how to incorporate user attributes from the metadata specification into a SAML 2.0 assertion.
SAML 2.0 Metadata Extension Schema	Defines a format by which to encode GFIPM entity attributes from the metadata specification within a GFIPM Trust Fabric file.
Sample GFIPM Trust Fabric File	Provides an example of how to incorporate entity attributes from the metadata specification into a GFIPM Trust Fabric file.

Table 1: GFIPM Metadata 2.0 Package Contents

4. Summary of Changes in Version 2.0

The Global Security Working Group (GSWG) released the GFIPM Metadata Specification, version 1.0, in 2008. Since that time, version 1.0 has been used in support of information

sharing activities within the National Information Exchange Federation (NIEF), an operational federation that comprises many GFIPM stakeholder agencies and employs GFIPM technology standards. The specification has also been used for other purposes, including information sharing activities within the CONNECT project, which enables law enforcement information sharing between several U.S. states. Lessons learned through operational experience in NIEF and CONNECT have led to various proposals for changes to the GFIPM Metadata Specification, and where feasible, these proposals have been incorporated into the GFIPM Metadata Specification, version 2.0.

The most significant change between versions 1.0 and 2.0 of the metadata is that version 2.0 uses a nonstructured, "flat" attribute model, whereas version 1.0 used a structured XML attribute model. Section 5 provides further details about this change, including the rationale for making the change.

In addition to the change from structured XML to flat attributes, the GFIPM Metadata Specification 2.0 incorporates many changes at the level of attribute content. Section 2 provides a description of the new attribute categories (resource attributes, action attributes, and environment attributes) that have been added to the specification. Within those new categories, several new attributes have been added to the specification. In addition, numerous changes have been made within the previously existing categories of user attributes and entity attributes. Table 2 provides a list of these attribute-level changes, including a description and rationale for each change.

Summary of Changes in GFIPM Metadata Specification 2.0		
Change ID	***Description of Change***	***Rationale for Change***
1	Add User Attribute: "NCIC Certification Indicator"	GFIPM Delivery Team member Rick Brown (FBI) pointed out that the metadata model does not contain information about this certification, which is important to many law enforcement officers.
2	Rename and Redefine User Attribute "NCIC Criminal History Certification Indicator" to "NCIC Criminal History Privilege Indicator"	GFIPM Delivery Team member Rick Brown (FBI) pointed out that there is no such thing as NCIC criminal history data "certification"; it is merely a privilege granted to some users under certain conditions.
3	Rename and Redefine User Attribute "NCIC Hotfile Certification Indicator" to "NCIC Hotfile Privilege Indicator"	GFIPM Delivery Team member Rick Brown (FBI) pointed out that there is no such thing as NCIC hotfile "certification"; it is merely a privilege granted to some users under certain conditions.

4	Rename and Redefine User Attribute "FBI IAFIS Certification Indicator" to "FBI IAFIS Privilege Indicator"	GFIPM Delivery Team member Rick Brown (FBI) pointed out that there is no such thing as FBI IAFIS "certification"; it is merely a privilege granted to some users under certain conditions.
5	Rename and Redefine User Attribute "FBI III Certification Indicator" to "FBI III Privilege Indicator"	GFIPM Delivery Team member Rick Brown (FBI) pointed out that there is no such thing as FBI III "certification"; it is merely a privilege granted to some users under certain conditions.
6	Rename and Redefine User Attribute "NICS File Certification Indicator" to "NICS File Privilege Indicator"	GFIPM Delivery Team member Rick Brown (FBI) pointed out that there is no such thing as NICS file "certification"; it is merely a privilege granted to some users under certain conditions.
7	Add User Attribute: "N-DEx Privilege Indicator"	GFIPM Delivery Team member Rick Brown (FBI) pointed out that the metadata model does not contain information about this privilege, which is important to many law enforcement officers.
8	Add User Attribute: "LEO Privilege Indicator"	GFIPM Delivery Team member Rick Brown (FBI) pointed out that the metadata model does not contain information about this privilege, which is important to many law enforcement officers.
9	Delete User Attribute: "DNA"	GTRI was unable to identify a standard encoding method for a person's DNA, and without a standard format in which to express the data, it is unclear how this data can be useful to a relying party.
10	Delete User Attribute: "Employer Organization ID"	The model already captures the user's employer's organization name and ORI code. Also, there is no clear guidance indicating the specific ID that this attribute should contain. It is therefore not usable.
11	Delete User Attribute: "Employment Status Text"	This attribute is not a code and has never been codified. It does not seem to be useful as a free-form field.
12	Delete User Attribute: "Employment Sworn Law Enforcement Officer Indicator"	This attribute has been a source of confusion for implementers since it first appeared. Also, the metadata model already accommodates assertion of the user's Sworn Law Enforcement Officer (SLEO) status separately from the user's employment information.

13	Delete User Attribute: "Employment Public Safety Officer Indicator"	This attribute has been a source of confusion for implementers since it first appeared. Also, the metadata model already accommodates assertion of the user's Public Safety Officer status separately from the user's employment information.
14	Delete User Attribute: "Employment Law Enforcement Involvement Category Code"	This code has only two values: "SLEO" and "Civilian". It is therefore redundant information, since the metadata model already has a SLEO indicator attribute.
15	Delete User Attribute: "Employment Assignment Start Date"	This attribute is nonsensical. A user is never "assigned" to an employer; a user is "employed" by an employer, and the metadata model already accommodates the user's hire date with his/her current employer.
16	Delete User Attribute: "Employment Assignment End Date"	This attribute is nonsensical. A user is never "assigned" to an employer; a user is "employed" by an employer. Also, there is no need to express a user's "employment end date" as part of his/her employment relationship, because the fact that the relationship is being asserted implies that the user is still employed.
17	Delete User Attribute: "Assignment Agency Organization ID"	The model already captures the user's assignment agency's name and ORI code. Also, there is no clear guidance indicating the specific ID that this attribute should contain. It is therefore not usable.
18	Delete User Attribute: "Authorized Purpose Text"	It is not possible for an IDP to make a meaningful assertion in "real time" about a specific action that a user is taking. This attribute therefore does not belong in a SAML assertion. It has been deleted as a user attribute and added as a new action attribute. (See below in this table.)
19	Delete User Attribute: "Identity Provider Organization ID"	The model already captures the user's identity provider organization's name and ORI code. Also, there is no clear guidance indicating the specific ID that this attribute should contain. It is therefore not usable.
20	Delete User Attribute: "Electronic Identity Serial Number"	This attribute is redundant; "Electronic Identity ID" already captures this concept.
21	Delete User Attribute: "Electronic Identity Signing Certificate"	The purpose of this attribute has never been clear. It is therefore not useful within the attribute model.

22	Delete User Attribute: "Electronic Identity Encryption Certificate"	The purpose of this attribute has never been clear. It is therefore not useful within the attribute model.
23	Delete User Attribute: "Electronic Identity Original Sponsoring Person Full Name"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
24	Delete User Attribute: "Electronic Identity Original Sponsoring Person E-mail Address Text"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
25	Delete User Attribute: "Electronic Identity Original Sponsoring Person Telephone Number"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
26	Delete User Attribute: "Electronic Identity Original Sponsoring Person Fax Number"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
27	Delete User Attribute: "Electronic Identity Current Sponsoring Person Full Name"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
28	Delete User Attribute: "Electronic Identity Current Sponsoring Person E-Mail Address Text"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.

29	Delete User Attribute: "Electronic Identity Current Sponsoring Person Telephone Number"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
30	Delete User Attribute: "Electronic Identity Current Sponsoring Person Fax Number"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
31	Delete User Attribute: "Electronic Identity Original Registering Person Full Name"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
32	Delete User Attribute: "Electronic Identity Original Registering Person E-Mail Address Text"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
33	Delete User Attribute: "Electronic Identity Original Registering Person Telephone Number"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
34	Delete User Attribute: "Electronic Identity Original Registering Person Fax Number"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
35	Delete User Attribute: "Electronic Identity Current Registering Person Full Name"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.

36	Delete User Attribute: "Electronic Identity Current Registering Person E-Mail Address Text"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
37	Delete User Attribute: "Electronic Identity Current Registering Person Telephone Number"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
38	Delete User Attribute: "Electronic Identity Current Registering Person Fax Number"	This information is typically stored by an IDP and could be disclosed to a relying party upon request during an audit. But it is not realistic to assume that IDPs will disclose this information as part of a SAML assertion, or that a relying party would derive value from this information at run-time.
39	Delete Entity Attribute: "Federation ID"	This attribute is not necessary because entity attribute data is used within a GFIPM Cryptographic Trust Fabric document that already requires and supports a means for uniquely identifying each entity.
40	Delete Entity Attribute: "Local ID"	This attribute is meaningless in the context of a GFIPM "entity," which is a trusted service endpoint.
41	Delete Entity Attribute: "Digital Signature"	This attribute is targeted towards software entities. But the current GFIPM concept of an "entity" is a trusted service endpoint. A digital signature does not apply to a software service endpoint in any way that is meaningful from a trust or security standpoint.
42	Delete Entity Attribute: "Full Name"	The GFIPM Cryptographic Trust Fabric document (within which entity attributes are asserted) already provides a facility for conveying an entity's full name.
43	Delete Entity Attribute: "Original Deployment Date"	The GFIPM Cryptographic Trust Fabric document (within which entity attributes are asserted) already provides a facility for conveying an entity's deployment date.

44	Delete Entity Attribute: "Expiration Date"	It is unclear what purpose an expiration date would serve for a GFIPM entity (trusted service endpoint). If its expiration date is related to its certificate's expiration date or the GFIPM Cryptographic Trust Fabric document's expiration date, then it is redundant. If it is not related to either of those expiration dates, then it has no clear purpose.
45	Delete Entity Attribute: "Primary Language Text"	This attribute is vague. It is not clear whether "language" conveys natural language (e.g., English) or a software programming language (e.g., Java). In either case, it is unclear why this information would be relevant to a secure software endpoint.
46	Delete Entity Attribute: "Version Text"	Since this attribute will appear in the GFIPM Cryptographic Trust Fabric and the trust fabric is a public document (posted at a public URL), it is unlikely that federation members will want to include implementation details about their software service entities (such as version number) in the trust fabric document. This attribute is therefore not useful.
47	Delete Entity Attribute: "Hash Value Text"	This attribute seems to be directed towards software entities. But the GFIPM concept of an "entity" is a trusted service endpoint. It is unclear how a hash value would apply to a service endpoint in a way that is meaningful from a trust or security standpoint. In addition, this attribute is vague. If the attribute is intended to support a digital hash for verification of a binary, then it is unclear what hash algorithm is to be used.
48	Delete Entity Attribute: "Primary Function Text"	It is unclear what type of "function" this attribute is supposed to capture. Also, an entity's primary function within a GFIPM federation should be clear from its entry in the GFIPM Cryptographic Trust Fabric, because it will be denoted as an identity provider, service provider, etc. This attribute is therefore unnecessary.
49	Delete Entity Attribute: "Category Text"	It is unclear what type of "category" this attribute is supposed to capture. It is therefore unnecessary.

50	Delete Entity Attribute: "Application Platform Text"	Since this attribute will appear in the GFIPM Cryptographic Trust Fabric and the trust fabric is a public document (posted at a public URL), it is unlikely that federation members will want to include implementation details about their software service entities (such as application platform) in the trust fabric document. This attribute is therefore not useful.
51	Delete Entity Attribute: "Build Number"	Since this attribute will appear in the GFIPM Cryptographic Trust Fabric and the trust fabric is a public document (posted at a public URL), it is unlikely that federation members will want to include implementation details about their software service entities (such as build number) in the trust fabric document. This attribute is therefore not useful.
52	Delete Entity Attribute: "Status Code"	The GFIPM Cryptographic Trust Fabric is distributed prior to run-time; therefore, it is not possible for the trust fabric to accurately know any type of transient status about an entity.
53	Delete Entity Attribute: "Owner Agency Organization ID"	The model already captures the entity's owner agency organization name and ORI code. Also, there is no clear guidance indicating the specific ID that this attribute should contain. It is therefore not usable.
54	Delete Entity Attribute: "Assignment Agency Name"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
55	Delete Entity Attribute: "Assignment Agency Organization ID"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
56	Delete Entity Attribute: "Assignment Agency Organization Category Code"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
57	Delete Entity Attribute: "Assignment Agency Organization General Category Code"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.

58	Delete Entity Attribute: "Assignment Agency Sub Unit Name"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
59	Delete Entity Attribute: "Assignment Agency Description Text"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
60	Delete Entity Attribute: "Assignment Agency ORI"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
61	Delete Entity Attribute: "Assignment Agency Street Address Text"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
62	Delete Entity Attribute: "Assignment Agency Post Office Box Text"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
63	Delete Entity Attribute: "Assignment Agency City Name"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
64	Delete Entity Attribute: "Assignment Agency County Code"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
65	Delete Entity Attribute: "Assignment Agency State Code"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
66	Delete Entity Attribute: "Assignment Agency Postal Code Text"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
67	Delete Entity Attribute: "Assignment Agency Country Code"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
68	Delete Entity Attribute: "Assignment Agency Primary Point of Contact Full Name"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.

69	Delete Entity Attribute: "Assignment Agency Primary Point of Contact E-Mail Address Text"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
70	Delete Entity Attribute: "Assignment Agency Primary Point of Contact Telephone Number"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
71	Delete Entity Attribute: "Assignment Agency Primary Point of Contact Fax Number"	Assignment of an entity (software service endpoint) from one agency to another is not a realistic scenario; therefore, this attribute is meaningless in a GFIPM federation.
72	Delete Entity Attribute: "Counter Terrorism Privilege Indicator"	The GFIPM concept of "local privileges" does not apply to the GFIPM concept of an "entity" as a software service endpoint.
73	Delete Entity Attribute: "Criminal History Privilege Indicator"	The GFIPM concept of "local privileges" does not apply to the GFIPM concept of an "entity" as a software service endpoint.
74	Delete Entity Attribute: "Criminal Investigative Privilege Indicator"	The GFIPM concept of "local privileges" does not apply to the GFIPM concept of an "entity" as a software service endpoint.
75	Delete Entity Attribute: "Criminal Intelligence Privilege Indicator"	The GFIPM concept of "local privileges" does not apply to the GFIPM concept of an "entity" as a software service endpoint.
76	Delete Entity Attribute: "Criminal Justice Privilege Indicator"	The GFIPM concept of "local privileges" does not apply to the GFIPM concept of an "entity" as a software service endpoint.
77	Delete Entity Attribute: "Government Privilege Indicator"	The GFIPM concept of "local privileges" does not apply to the GFIPM concept of an "entity" as a software service endpoint.
78	Delete Entity Attribute: "Public Privilege Indicator"	The GFIPM concept of "local privileges" does not apply to the GFIPM concept of an "entity" as a software service endpoint.
79	Delete Entity Attribute: "Commercial Privilege Indicator"	The GFIPM concept of "local privileges" does not apply to the GFIPM concept of an "entity" as a software service endpoint.
80	Delete Entity Attribute: "Test Privilege Indicator"	The GFIPM concept of "local privileges" does not apply to the GFIPM concept of an "entity" as a software service endpoint.
81	Delete Entity Attribute: "Subscriber Privilege Indicator"	The GFIPM concept of "local privileges" does not apply to the GFIPM concept of an "entity" as a software service endpoint.

82	Delete Entity Attribute: "Authorized Purpose Text"	It is not possible for a federation manager organization (which asserts attributes about entities in a GFIPM federation) to make a meaningful assertion in real time about a specific action that an entity is taking, since entity attribute data is distributed prior to run-time as part of the GFIPM Cryptographic Trust Fabric. This attribute therefore does not belong in an assertion about an entity.
83	Delete Entity Attribute: "Owner Agency Primary Point of Contact Full Name"	This attribute is being removed in favor of three similar entity attributes from the SAML 2.0 Metadata specification. These new attributes describe the full name(s) of the entity's administrative, technical, and support points of contact.
84	Delete Entity Attribute: "Owner Agency Primary Point of Contact E-Mail Address Text"	This attribute is being removed in favor of three similar entity attributes from the SAML 2.0 Metadata specification. These new attributes describe the e-mail address(es) for the entity's administrative, technical, and support points of contact.
85	Delete Entity Attribute: "Owner Agency Primary Point of Contact Telephone Number"	This attribute is being removed in favor of three similar entity attributes from the SAML 2.0 Metadata specification. These new attributes describe the phone number(s) for the entity's administrative, technical, and support points of contact.
86	Delete Entity Attribute: "Owner Agency Primary Point of Contact Fax Number"	This attribute is being removed in favor of three similar entity attributes that describe the fax number(s) for the entity's administrative, technical, and support points of contact.
87	Add User Attribute: "Emergency Contact Full Name"	This attribute is part of the HSPD-12 Backend Attribute Exchange (BAE) attribute model and appears to be a valuable addition to the GFIPM Metadata Specification.
88	Add User Attribute: "Emergency Contact Telephone Number"	This attribute is part of the HSPD-12 Backend Attribute Exchange (BAE) attribute model and appears to be a valuable addition to the GFIPM Metadata Specification.
89	Add User Attribute: "Emergency Contact E-Mail Address"	This attribute is part of the HSPD-12 Backend Attribute Exchange (BAE) attribute model and appears to be a valuable addition to the GFIPM Metadata Specification.

90	Add User Attribute: "NIPP Sector Code"	This attribute is part of the HSPD-12 Backend Attribute Exchange (BAE) attribute model and appears to be a valuable addition to the GFIPM Metadata Specification. Note that NIPP = "National Infrastructure Protection Plan."
91	Add User Attribute: "Emergency Support Function Code"	This attribute is part of the HSPD-12 Backend Attribute Exchange (BAE) attribute model and appears to be a valuable addition to the GFIPM Metadata Specification.
92	Add User Attribute: "Employment Management Level"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification. The original motivation for this attribute came from the DHS Attribute-Based Access Control (ABAC) Report.
93	Add User Attribute: "Employment Jurisdiction"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification. The original motivation for this attribute came from the DHS Attribute-Based Access Control (ABAC) Report.
94	Add User Attribute: "Assignment Jurisdiction"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification. The original motivation for this attribute came from the DHS Attribute-Based Access Control (ABAC) Report.
95	Add Entity Attribute: "Entity ID"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.
96	Add Entity Attribute: "Description"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its practical value in providing a "plain-English" description of an entity.
97	Add Entity Attribute: "Technical Role"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its practical value in providing a standard representation for the type of technical role(s) played by an entity in a federation.

98	Add Entity Attribute: "Certificate"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.
99	Add Entity Attribute: "Administrative Point of Contact Full Name"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.
100	Add Entity Attribute: "Administrative Point of Contact E-mail Address Text"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.
101	Add Entity Attribute: "Administrative Point of Contact Telephone Number"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.
102	Add Entity Attribute: "Administrative Point of Contact Fax Number"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its applicability as a means for reaching a point of contact for an entity.
103	Add Entity Attribute: "Technical Point of Contact Full Name"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.
104	Add Entity Attribute: "Technical Point of Contact E-Mail Address Text"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.

105	Add Entity Attribute: "Technical Point of Contact Telephone Number"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.
106	Add Entity Attribute: "Technical Point of Contact Fax Number"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its applicability as a means for reaching a point of contact for an entity.
107	Add Entity Attribute: "Support Point of Contact Full Name"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.
108	Add Entity Attribute: "Support Point of Contact E-mail Address Text"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.
109	Add Entity Attribute: "Support Point of Contact Telephone Number"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its inclusion in the SAML 2.0 Metadata Specification, which is used as the normative specification for the GFIPM Trust Fabric.
110	Add Entity Attribute: "Support Point of Contact Fax Number"	The GFIPM Delivery Team identified this attribute as a valuable addition to the GFIPM Metadata Specification based on its applicability as a means for reaching a point of contact for an entity.
111	Add Resource Attribute: "Counter Terrorism Data Indicator"	The GFIPM Delivery Team identified this attribute as a potentially valuable indicator for categorizing data resources for the purpose of defining XACML-style access control policies.
112	Add Resource Attribute: "Criminal History Data Indicator"	The GFIPM Delivery Team identified this attribute as a potentially valuable indicator for categorizing data resources for the purpose of defining XACML-style access control policies.
113	Add Resource Attribute: "Criminal Investigative Data Indicator"	The GFIPM Delivery Team identified this attribute as a potentially valuable indicator for categorizing data resources for the purpose of defining XACML-style access control policies.

114	Add Resource Attribute: "Criminal Intelligence Data Indicator"	The GFIPM Delivery Team identified this attribute as a potentially valuable indicator for categorizing data resources for the purpose of defining XACML-style access control policies.
115	Add Resource Attribute: "Criminal Justice Data Indicator"	The GFIPM Delivery Team identified this attribute as a potentially valuable indicator for categorizing data resources for the purpose of defining XACML-style access control policies.
116	Add Resource Attribute: "Government Data Indicator"	The GFIPM Delivery Team identified this attribute as a potentially valuable indicator for categorizing data resources for the purpose of defining XACML-style access control policies.
117	Add Resource Attribute: "Public Data Indicator"	The GFIPM Delivery Team identified this attribute as a potentially valuable indicator for categorizing data resources for the purpose of defining XACML-style access control policies.
118	Add Resource Attribute: "Commercial Data Indicator"	The GFIPM Delivery Team identified this attribute as a potentially valuable indicator for categorizing data resources for the purpose of defining XACML-style access control policies.
119	Add Resource Attribute: "Test Data Indicator"	The GFIPM Delivery Team identified this attribute as a potentially valuable indicator for categorizing data resources for the purpose of defining XACML-style access control policies.
120	Add Resource Attribute: "Subscriber Data Indicator"	The GFIPM Delivery Team identified this attribute as a potentially valuable indicator for categorizing data resources for the purpose of defining XACML-style access control policies.
121	Add Action Attribute: "Action Type"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information about an information sharing transaction for the purpose of defining XACML-style access control policies.
122	Add Action Attribute: "Authorized Purpose"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information sharing transaction for the purpose of defining XACML-style access control policies. Note that "Authorized Purpose" previously existed as both a user attribute and an entity attribute. Both of those attributes have been deleted, since the concept was not applicable in those attribute categories.

123	Add Action Attribute: "Geolocation Latitude"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information about an information sharing transaction for the purpose of defining XACML-style access control policies.
124	Add Action Attribute: "Geolocation Longitude"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information about an information sharing transaction for the purpose of defining XACML-style access control policies.
125	Add Environment Attribute: "Homeland Security Threat Level"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information about the environment within which an information sharing transaction can occur.
126	Add Environment Attribute: "Date Time"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information about the environment within which an information sharing transaction can occur.
127	Add Environment Attribute: "Local Weather Conditions"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information about the environment within which an information sharing transaction can occur.
128	Add User Attribute: "Passport ID"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information about some users.
129	Add User Attribute: "Passport Country Code"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information about some users.
130	Add User Attribute: "Visa Category"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information about some users.
131	Add User Attribute: "Visa Number Text"	The GFIPM Delivery Team identified this attribute as a potentially valuable source of information about some users.

Table 2: List of Changes in GFIPM Metadata 2.0

5. Rationale for Change From XML to Flat Attribute Model

As noted in Section 4, the biggest change between versions 1.0 and 2.0 of the GFIPM Metadata Specification is that version 2.0 uses a "flat" attribute model to represent metadata attributes. In contrast, version 1.0 of the specification used a structured XML attribute model. This section provides some insight into the rationale for making this significant change to the standard.

The GFIPM program began in 2005 as the GFIPM Security Interoperability Demonstration Project, which lasted about 18 months and resulted in the implementation of an operational, information sharing federation based on the SAML[1] standard. The demonstration project also resulted in the development of an early version of the GFIPM Metadata Specification. At that time, demonstration project participants believed that the metadata standard should be designed for close alignment with NIEM.[2] Accordingly, early "point releases" (versions 0.1 through 0.4) of the GFIPM Metadata, as well as version 1.0 of the standard, used a "complex XML" format similar to the structure of NIEM data objects.

Implementation experience over the last several years has provided evidence that the decision to adopt NIEM's XML structure into the GFIPM Metadata Specification was misguided, for two reasons. First, structured XML content tends to introduce unnecessary complexity, including the need for custom code, in most SAML COTS products. Second, the systems that process GFIPM Metadata assertions do not typically derive any benefit from user attribute information in an XML structure; on the contrary, such a complex structure usually requires custom code to disassemble the XML into its constituent "flat" attributes. It is now clear that representing GFIPM Metadata attributes in XML format introduces complexity without tangible benefits.

To rectify this problem, the GFIPM Delivery Team chose to simplify the representation structure of the GFIPM Metadata for version 2.0. The metadata structure is now a "flat" list of attributes. This flat structure is much more practical for use within SAML COTS products. The change from structured XML to a flat list of attributes does carry a sacrifice in the expressiveness of the data model; however, this sacrifice is minimal and is unlikely to affect users of the model in most usage scenarios. The corresponding benefit in complexity reduction and compatibility with COTS products is significant.

6. SAML Assertion Encoding Rules for User Attributes

At the time of the release of the GFIPM Metadata Specification 2.0, the primary use case for GFIPM user attributes is the transmission of information about a user within a SAML assertion, from an asserting party (often called an Identity Provider) to a relying party (often called a Service Provider). The GFIPM Web Browser User-to-System Profile[3] calls for the use of a signed SAML 2.0 assertion as the format through which these user attributes are passed from asserting party to relying party.

[1] The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between identity providers and service providers within a federated environment. SAML is a product of the OASIS Security Services Technical Committee (SSTC).

[2] The National Information Exchange Model (NIEM) is an XML-based information exchange framework developed by Global.

[3] The GFIPM Web Browser User-to-System Profile, version 1.1, is a GFIPM normative technical specification that addresses interoperability for the use case in which a user accesses Web-based services via a Web browser, using the SAML 2.0 Single Sign-On (SSO) Profile for secure transmission of attributes about the user from the user's Identity Provider to a Service Provider.

The following guidelines provide an informal description of how to encode GFIPM Metadata 2.0 user attributes within a SAML 2.0 assertion.

1. Within the XML structure of a SAML 2.0 Assertion, the **<saml:Assertion>** element contains a **<saml:AttributeStatement>** element, and the **<saml:AttributeStatement>** element contains zero or more **<saml:Attribute>** elements.

2. Each **<saml:Attribute>** element must correspond to exactly one GFIPM user attribute. A **<saml:Attribute>** element has an XML attribute called "**Name**" to denote the application-level name of the attribute. This "**Name**" XML attribute must contain the full formal name of the GFIPM Metadata user attribute to which this **<saml:Attribute>** element corresponds.

3. Each **<saml:Attribute>** element has an optional XML attribute called "**NameFormat**" For each "saml:Attribute" element that corresponds to a GFIPM user attribute, this "NameFormat" XML attribute must be present, and its value must be "**urn:oasis:names:tc:SAML:2.0:attrname-format:uri**".

4. Each **<saml:Attribute>** element that corresponds to a GFIPM user attribute must contain exactly one **<saml:AttributeValue>** element. The data contained within the **<saml:AttributeValue>** element must correspond to the value of the GFIPM user attribute represented by its enclosing **<saml:Attribute>** element.

Figure 1 contains a sample **<saml:Attribute>** element corresponding to the GFIPM user attribute "**gfipm:2.0:user:FederationId**". Note that the **<saml:AttributeValue>** element contains additional XML attributes ("**xmlns:xsi**" and "**xsi:type**") that are not mentioned above. These attributes are necessary and would be explicitly required by a normative specification for encoding GFIPM user attributes within a SAML assertion; however, they are not called out in the encoding rules above because the rules described in this document are not normative.

```
<saml:Attribute Name="gfipm:2.0:user:FederationId"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml:AttributeValue
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">
    GFIPM:IDP:JNET:USER:johndoe@jnet.net
  </saml:AttributeValue>
</saml:Attribute>
```

Figure 1: Sample <saml:Attribute> Element

7. Trust Fabric Encoding Rules for Entity Attributes

In addition to user attributes, the GFIPM Metadata Specification includes a set of entity attributes. These entity attributes have existed within the GFIPM Metadata Specification since the first point release of the model in 2006; however, prior to version 2.0, these entity attributes have never been used. Throughout much of the early GFIPM work, it was not clear exactly what constituted an "entity." However, recent work on GFIPM Web services has provided a clearer understanding of what the term "entity" means within GFIPM: *an entity is a trusted software service endpoint within a federation*.

Just as it is possible to assert facts (attributes) about a user within a federation, it is also possible to assert facts about a software service endpoint. But there are differences between the assertion of user attributes and entity attributes. The most important difference is the party in the federation that makes the assertions. The party that makes an assertion about a user is the user's identity provider. But the party that makes an assertion about an entity is the federation manager. The federation manager can make a trusted third-party statement (assertion) about an entity for the benefit of other entities in the federation, just as a user's identity provider can make a trusted third-party statement about a user for the benefit of relying parties in the federation.
Since the federation manager is responsible for asserting trusted information about entities, the most appropriate place in which to make those assertions is within the federation's GFIPM Cryptographic Trust Fabric document. The following guidelines provide an informal description of how to encode GFIPM Metadata 2.0 entity attributes within a GFIPM Cryptographic Trust Fabric document.

1. Within the XML structure of a GFIPM Cryptographic Trust Fabric document, the following element types may contain a **`<md:Extensions>`** element: "**`md:EntityDescriptor`**", "**`md:Organization`**", "**`md:IDPSSODescriptor`**", and "**`md:SPSSODescriptor`**".

2. Within a GFIPM Cryptographic Trust Fabric document, a **`<md:Extensions>`** element can contain any type of XML content as defined in an extension schema.[4] To encode GFIPM entity attribute data, the **`<md:Extensions>`** element may contain zero or more **`<gfipm:EntityAttribute>`** elements.

3. Each **`<gfipm:EntityAttribute>`** element must correspond to exactly one GFIPM entity attribute. A **`<gfipm:EntityAttribute>`** element has an XML attribute called "**`Name`**" to denote the GFIPM name of the attribute. This "**`Name`**" XML attribute must contain the full formal name of

[4] The XML extension schema file for encoding GFIPM entity attributes within a GFIPM Cryptographic Trust Fabric document is included in the GFIPM Metadata 2.0 specification.

the GFIPM Metadata entity attribute to which this **<gfipm:EntityAttribute>** element corresponds.

4. Each **<gfipm:EntityAttribute>** element has a mandatory XML attribute called "**NameFormat**". For each **<gfipm:EntityAttribute>** element that corresponds to a GFIPM entity attribute, this "**NameFormat**" XML attribute must be present, and its value MUST be "**urn:oasis:names:tc:SAML:2.0:attrname-format:uri**".

5. Each **<gfipm:EntityAttribute>** element that corresponds to a GFIPM entity attribute must contain exactly one **<gfipm:EntityAttributeValue>** element. The data contained within the **<gfipm:EntityAttributeValue>** element MUST correspond to the value of the GFIPM entity attribute represented by its enclosing **<gfipm:EntityAttribute>** element.

Figure 2 contains a sample **<gfipm:EntityAttribute>** element corresponding to the GFIPM entity attribute "**gfipm:2.0:entity:OwnerAgencyORI**". Note that the **<gfipm:EntityAttributeValue>** element contains additional XML attributes ("**xmlns:xsi**" and "**xsi:type**") that are not mentioned above. These attributes are necessary and would be explicitly required by a normative specification for encoding GFIPM entity attributes within a GFIPM Cryptographic Trust Fabric document; however, they are not called out in the encoding rules above because the rules described in this document are not normative.

```
<gfipm:EntityAttribute
    Name="gfipm:2.0:entity:OwnerAgencyORI"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    xmlns:gfipm="http://gfipm.net/metadata/entity/2.0">
  <gfipm:EntityAttributeValue
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">
    GA012345
  </gfipm:EntityAttributeValue>
</gfipm:EntityAttribute>
```

Figure 2: Sample <gfipm:EntityAttribute> Element

8. Encoding and Use of New Attribute Categories

As described in Section 2, this version of the specification contains three new categories of attributes: resource attributes, action attributes, and environment attributes. These new attribute categories have not yet been used within experimental or operational systems by GFIPM stakeholders; therefore, this specification does not provide any guidance for the

encoding or use of these new attribute categories.[5] Future versions of this specification will address this topic.

9. Metadata Extensions and Changes

The GFIPM Metadata Specification is a work in progress and will no doubt undergo many revisions during its lifetime. The goal of the GSWG is for the metadata model to grow and evolve based on the changing needs of GFIPM stakeholders. The following guidelines serve to accommodate the necessary changes that may occur to the metadata model over time.

Temporary Extensions to the Metadata Model for Local Use

Occasionally, users of the GFIPM Metadata Specification may find it necessary to augment the metadata model with one or more additional attributes, to make the model more useful within a particular federation or among a group of organizations within a federation. When defining an extension attribute, follow these rules.

1. Use a name within one of the following namespaces as appropriate based on the attribute category of the new attribute: "**`gfipm:ext:user`**" for a user attribute, "**`gfipm:ext:entity`**" for an entity attribute, "**`gfipm:ext:resource`**" for a resource attribute, "**`gfipm:ext:action`**" for an action attribute, and "**`gfipm:ext:environment`**" for an environment attribute.

2. Choose an appropriate data type for the attribute. Use a code set if the attribute is intended for use in access control decisions. If an appropriate code set exists (e.g., through FIPS, NIST, NIEM), reuse it rather than defining a new code set.

3. Choose an attribute name that concisely conveys the attribute's meaning.

4. Provide a clear definition for the attribute. An attribute without a clear definition is usually not valuable.

5. Provide usage guidance for the attribute if appropriate.

[5] As noted in Section 2, one of the motivators for the inclusion of the new attribute categories is to align the GFIPM Metadata Specification with the requirements of the eXtensible Access Control Markup Language (XACML) specification. It is expected that future work with XACML by GFIPM stakeholders will lead to insights and guidance about how to best use these new attribute categories within the context of XACML and other access management technologies.

Proposing Changes to the GFIPM Metadata Specification

While local extensions to the metadata model can prove valuable for small groups of organizations, such extensions do not provide any benefit to the broader GFIPM stakeholder community. To maximize the utility of the GFIPM Metadata Specification for every organization that uses it, the GSWG requests that all GFIPM stakeholders exercise diligence in submitting change requests for the metadata model, to ensure that it evolves as needed to meet the needs of the GFIPM community.

There are three types of change requests that stakeholders can submit.

1. ***Addition of Attribute—***This is a request to add a new attribute to the metadata model.

2. ***Deletion of Attribute—***This is a request to delete or deprecate an existing attribute that does not appear to be of value to users of the metadata model.

3. ***Definitional Change—***This is a request to change or clarify the definition of an attribute in the metadata model.

Please submit all change requests to John Wandelt, Georgia Tech Research Institute, at john.wandelt@gtri.gatech.edu.

Versioning Strategy for GFIPM Metadata Specification

Over time, in response to change requests from GFIPM stakeholders, it may be necessary for GSWG to release subsequent versions of this specification. To permit the release of additional metadata versions while minimizing the impact on organizations implementing the specification, the following versioning strategy is in place.

1. Starting with version 2.0, each attribute in the specification contains its own version number. An attribute's version number is contained within its full formal name. For example, the attribute "**`gfipm:2.0:user:FederationId`**" has version number 2.0.

2. After an attribute has been defined, its name, definition, data type, and version number will *never* change. A subsequent request to change its definition may result in the creation of a new attribute with a new definition; however, the old attribute will continue to persist within the metadata model for legacy use by implementers. At some point, an attribute may be deleted because it has been superseded by an updated attribute that is more precise or better suited to the community's needs;

however, the decision to delete an attribute is separate from the decision to add a new attribute that may supersede it.

3. Subsequent releases of the GFIPM Metadata Specification will be versioned according to the highest attribute version number among all the attributes contained in that version of the specification. For example, in version 2.0 of the specification, every attribute is versioned at 2.0. When version 2.1 of the specification is released, it will contain one or more new attributes with version 2.1, as well as attributes versioned at 2.0 that have been carried over from version 2.0 of the specification. This specification versioning strategy allows for incremental extension to the specification without requiring implementers to make changes to operational systems, unless they want to take advantage of changes made in the new version of the specification.

10. Feedback

As discussed in previous sections, the GFIPM metadata specification is expected to undergo additional iterations over the coming years. Comments and feedback from a broader community of reviewers are necessary to broaden the perspective beyond the requirements of the contributors that led to the current version. Sufficient work has been accomplished and documented in the accompanying file set to solicit constructive comments to help shape future versions of this specification. The Global Security Working Group requests that comments be submitted directly to John Wandelt, Georgia Tech Research Institute, at john.wandelt@gtri.gatech.edu. Comments will be compiled, reconciled, and scheduled for review as part of the GSWG GFIPM work plan.

About Global

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

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

www.it.ojp.gov/gfipm

or call

(850) 385-0600