Global Federated Identity and Privilege Management (GFIPM) Metadata Overview Version 1.0

By: Global Justice Information Sharing Initiative (Global) Security Working Group

February 11, 2008

This project was supported by Grant No. 2005-NC-BX-K164 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.

Table of Contents

Acknowledgements

The Global Federated Identity and Privilege Management (GFIPM) initiative is supported by joint funding of the United States Department of Homeland Security (DHS) and the United States 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, who 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 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, http://it.ojp.gov/GFIPM, for official announcements.

Members of the GFIPM Delivery Team

Rick Brown, FBI

Jim Douglas, SEARCH

James Dyche, JNET (past member)

Glen Gillum, CISA

Larry Maloney, RISS

Christina Rogers, California DOJ

John Ruegg, Los Angeles County ISAB

Pam Scanlon, ARJIS

Martin Smith, DHS

John Wandelt, GTRI

Members of the Technical Privacy Task Team

Joeseph Aldaheff, Oracle

Jim Cabral, IJIS

Alan Carlson, The Justice Management Institute

Scott Fairholm, NCSC

Owen Greenspan, SEARCH

Alan Harbitter, IJIS

Erin Kenneally, eLCHEMY

Joe Mierwa, IJIS

John Ruegg, Los Angeles County ISAB

Chelle Uecker, Superior Court of California

John Wandelt, GTRI

Other Primary Contributors and Collaborators

James Dyche, JNET

John Davenport, JNET

Bob Greeves, BJA

Patricia Hammer, DHS

Tom Kooy, JusticeExperts.com

Jeff Krug, GTRI

Christina Medlin, GTRI

Matt Moyer, GTRI

Stefan Roth, GTRI

Lisa Sills, GTRI

Chris Traver, BJA

Karen Waterman, DHS

David Woolfenden

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. Just as a common XML data model was the key to data interoperability, a standard XML set of security attributes about federations' or users' identities, privileges, and authentication details can be universally communicated. 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.

This document and the associated GFIPM Metadata Package 1.0 define common semantics and structure for metadata describing *federated users* and other *federated entities* (hosts, devices, services, etc.) essential to the GFIPM concept. This metadata can be used in support of identification, authentication, privilege management/access control/authorization, auditing, and personalization across a federation. A layered framework and approach are presented that distinguish between the GFIPM metadata content itself and the methods for encoding and transporting that metadata in Security Assertion Markup Language (SAML) assertions.

This document does *not* contain information about the actual contents of the GFIPM Metadata Package 1.0. The package itself provides that information via the following artifacts.

Artifact	Description
Metadata Overview Document	This document
XML Schemas	Contain the official schema-level specification of the metadata model
Microsoft Excel Spreadsheets	Contain a hyperlinked, browsable representation of the metadata model, including definitions and usage guidance for each metadata attribute
UML-Style Diagram Images	Contain a visual representation of the metadata model
SAML 2.0 Encoding Rules Document	Contains rules for encoding GFIPM Metadata for transport via SAML 2.0
Sample XML Instances	Provide examples of valid XML that conform to the metadata schemas

The GFIPM metadata has been developed based on data requirements and feedback from Global Security Working Group (GSWG) members and GFIPM Security Interoperability Demonstration Project[1] participants. 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.

[1] See the GFIPM Security Interoperability Demonstration Project Report for more information.

2. Metadata Modeling: Leveraging GJXDM/NIEM

Given the work and success of the Global Justice XML Data Model (GJXDM) and the National Information Exchange Model (NIEM) data-modeling efforts, it is logical to leverage and reuse these specifications in the GFIPM metadata. Leveraging NIEM inherently makes the GFIPM metadata model immediately more applicable to other domains and systems, rather than focused only on criminal justice users and systems. Design requirements for the GFIPM metadata include the following:

- Identify the attributes needed to support the business use cases for interoperable federated identity and privilege management within the criminal justice community.
- Identify the standard technology and representation for these attributes.
- Define the "assertion" structure for the technology employed.

The GFIPM metadata design includes metadata supporting four major capabilities, or use cases. Each capability is described as follows:

- ***Identification/Authentication*—**Metadata needed to communicate identification of end users and the associated authentication context. Who is the end user and how did the user authenticate?
- ***Privilege Managemen*t—**Metadata captured by identity providers (IDPs) that can assist service providers (SPs) in making authorization decisions. What certifications, clearances, job functions, local privileges, organizational affiliations, etc., are associated with the end user that can serve as the basis for authorization decisions?
- ***Auditing*—**Metadata needed or required for the purposes of auditing systems, system access, business use, and legal compliance.
- ***Personalization*—**Metadata that can enable local systems to feature "specialized" services, regionalization, or special interest characteristics of their local software (e.g., regional news or alerts, SIG information, and display and tool settings or preferences).

3. GFIPM Metadata Design Process

A bottom-up approach was used in the identification and development of the GFIPM metadata based on actual requirements of operational systems of contributing members. The development and testing of the GFIPM model were based on a limited scope. The primary focus was on the collection of attributes (metadata) required to support the GFIPM use cases and specify federated users and federated entities in accordance with known and applicable industry standards. Scope was initially limited to responses provided by Global Security Working Group (GSWG) survey participants.

The GFIPM metadata was developed based on feedback from GFIPM demonstration project participants and others. At the time of this writing in December 2007, Version 0.4 of the metadata is currently in operational use by the GFIPM participants and has been since March 2007. The GFIPM Metadata 1.0 represents further refinement of Version 0.4. It also reflects input from the broader justice community, and it has been updated to use NIEM Version 2.0.

By including metadata about both users and nonhuman entities, the GFIPM metadata model supports the necessary attributes for system-to-system, user-to-system, and user-to-user use cases for information sharing. The specific metadata requirements of any of these use cases can be met by defining a profile, or subset, of the GFIPM metadata model. It should be noted, however, that a comprehensive collection of all security metadata requirements needed for the justice or national information sharing community—including privacy, Service-Oriented Architecture (SOA), networking, other layers of the security stack, and a comprehensive security process—was outside the scope of this initial metadata specification.

Table 1 provides a summary of the process through which the GFIPM metadata was developed and vetted. It also includes items that have yet to be completed.

GFIPM Metadata Development Process		
Process	**Description**	**Status**
Advanced vetting of the GFIPM metadata	Broader vetting of the GFIPM metadata is required. The GSWG and Global community will continue to serve as the vehicle for this expanded vetting of the GFIPM.	Ongoing since March 2006
Harmonize with current version of NIEM	After consensus had been reached on the data requirements, semantics, and representation of the GFIPM metadata, it was semantically and structurally harmonized with the current version of NIEM, which was version 2.0.	Completed (October 2007)
Incorporate feedback and iteratively refine GFIPM metadata	The current version of the GFIPM metadata is 1.0. Based on feedback from the vetting process and additional lessons learned, new versions of the GFIPM metadata package will be published as needed. A GFIPM delivery team was established in September 2007 to facilitate the operational adoption of GFIPM. This includes serving as the configuration management authority over the GFIPM metadata specification.	Ongoing since October 2007

Develop and vet GFIPM assertion specification	A set of alternatives for encoding the GFIPM metadata in SAML, along with pros and cons, has been identified and documented. The GFIPM demonstration project participants reviewed these alternatives and selected one for use in the demonstration project. Lessons learned were captured from the demonstration project, leading to further specification and recommendations for the GFIPM metadata. Additionally, specific encoding techniques have implications with regard to COTS product support. Some limited COTS testing has been conducted as part of the demonstration product. Lessons learned have been captured and have led to a new recommendation for encoding the GFIPM Metadata 1.0 for transport with SAML 2.0.	Completed (December 2007)
Specify other layers of the GFIPM specification	While this document lays out a four-layer framework for GFIPM metadata, there are also other aspects of interoperability that need to be defined within the GFIPM concept. There is a parallel effort currently ongoing to define a more general GFIPM Interoperability Specification that will address these issues.	Publish Q1 2008
Collect additional metadata requirements	The current version of the GFIPM metadata was derived from a fairly small set of survey participants and a limited amount of usage experience within the U.S. Department of Homeland Security (DHS)/U.S. Department of Justice (DOJ) GFIPM Security Interoperability Demonstration Project. It is expected to expand with additional inputs as new requirements are identified and submitted for inclusion.	Ongoing since March 2006
Create and update metadata definitions as needed	Many of the definitions associated with the metadata need to be expanded with input from domain experts and authoritative sources.	Ongoing since March 2006
Provide code tables where necessary	Some properties are currently of type “text” and should more appropriately be specific codes to facilitate automated authorization decisions by service providers. However, an authoritative code table either does not exist or has not been identified yet and may have to be developed.	Ongoing since March 2006

Map GFIPM to Justice Reference Architecture (JRA) and SOA	We need to determine where and how the GFIPM concept and GFIPM specifications can be leveraged in the JRA framework and, in general, an SOA (i.e., system-to-system use case). One such possibility is the reuse of the GFIPM metadata conceptual model and associated schemas. These are designed in a manner independent of the transport mechanism (SAML here) and can be leveraged directly by other components of the overall architecture (e.g., Web services and other IEPDs).	Ongoing; we need to continue to coordinate activities through GSWG with JRA/SOA team leads.

Table 1: GFIPM Metadata Development Process

4. GFIPM Metadata Framework

This section describes a framework used to define flexible and reusable concepts of a federated user and a federated entity for federated identity and privilege management. The framework has the following primary objectives.

- Leverage the existing GJXDM and NIEM data modeling concepts, principles, architecture, and content (semantics and structure).

- Leverage existing federated identity standards, especially the Security Assertion Markup Language (SAML). Support for other standards and versions is anticipated in the future, as those standards and versions become relevant to Global's mission.

- Separate the identification and modeling of GFIPM metadata from the encoding and transport of that metadata using SAML. This allows for parallel efforts to occur on both the business aspects of the metadata and the specific technical details related to protocol-level encoding.

Figure 1 depicts the four layers of the framework. Each layer has a distinct purpose and representation, as explained below.

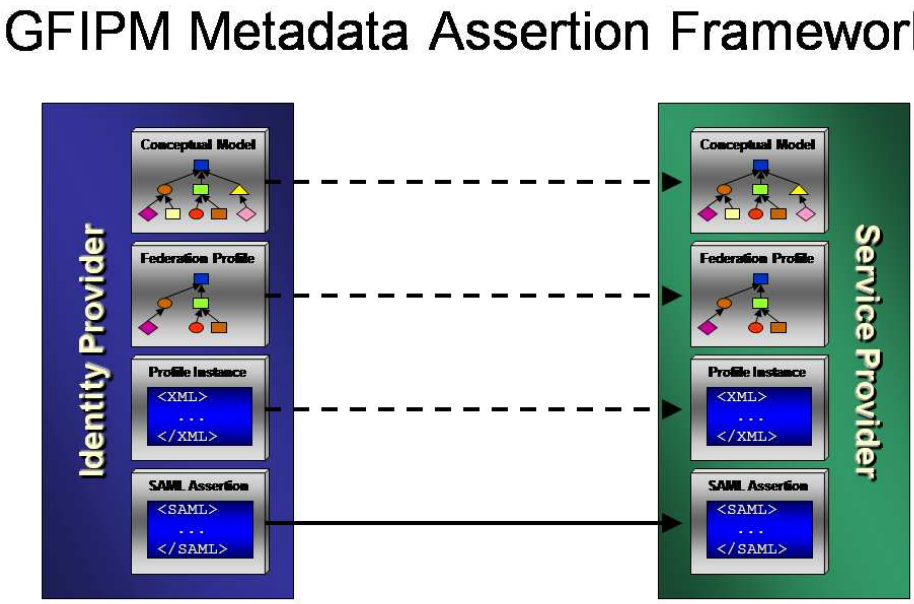

Figure 1: GFIPM Metadata Assertion Framework

4.1 The Conceptual Model Layer

At the highest layer of the framework is the *conceptual model*. A well-defined, standardized conceptual data model of a federated user or entity is essential to the GFIPM concept. Without a standardized data model, even simple concepts—such as "name," "employment," and "job title"—can introduce ambiguity when they are used and shared across organizational boundaries. The conceptual model provides clear structure, semantics, and relationships of properties associated with a federated user. It is independent of the underlying transport protocol and representation used to move federated user metadata between identity providers (IDPs) and service providers (SPs).

In addition to the concept of a federated user, the conceptual model also defines the concept of a federated entity, which is any nonhuman object (e.g., hardware, software, organization name, and service) that exists within a federation and requires a federated identity.

As stated previously, the GFIPM metadata leverages NIEM for its base vocabulary, as well as naming and design rules for describing the conceptual model and building the associated schemas. However, NIEM does not currently include the concept of a federated user or a federated entity; therefore, these concepts are defined here.

The following principles were applied in the construction of the conceptual model:

- ***Optional and Over-Inclusive***: The conceptual model is designed to act as a superset of the federated user or federated entity model that a typical

federation would adopt for its use. It includes many concepts that may have limited or no applicability in one federation and be critical concepts in another federation. By being optional and over-inclusive, the GFIPM conceptual model can address the data-modeling requirements of many different federations, thereby achieving maximum flexibility and reusability.

- ***Leverage NIEM***: The conceptual model leverages existing NIEM data model standards as much as possible. This helps to minimize the development effort for the federated user and federated entity data models, leverage the existing knowledge base, and promote interoperability with existing systems and tools that have been built around the NIEM standard.

- ***Leverage Existing Standards***: Many of the data requirements for the federated user and federated entity conceptual models have been identified in existing standards that address the generic federated identity and privilege management problem. Where attributes have been identified as part of a broader industry standard, they are referenced in the context of the existing standard rather than being redefined.

- ***Supplement Existing Standards Where Necessary***: The NIEM standard forms a critical part of the federated user and federated entity models; however, it does not include all of the concepts that are necessary for federated identity and privilege management. The federated user and federated entity models supplement NIEM by defining their own objects that represent extensions or additions to the NIEM vocabulary.

The conceptual model layer is formally specified via three XML schemas. There is also a Microsoft Excel spreadsheet available for easier readability, including a definition for each element, usage guidance where necessary, and references to the appropriate NIEM and SAML structures where necessary.

4.2 The Federation Profile Layer

The *federation profile* layer allows the conceptual model to be subsetted and constrained for a given federation implementation. It serves as an adapter layer, allowing a federation to distill the general federated user and federated entity models down to an essential supported set of elements. In addition to specifying a subset of the larger model, a federation profile can specify constraints and mandatory elements. The federation profile layer is formally specified by a set of schemas that specify a subset of the schemas used to define the conceptual model layer. The GFIPM federation is currently using one particular federation profile; however, as previously stated, this specific profile is only one of many possible federation profiles that can be derived from the GFIPM metadata conceptual model.

4.3 The Federation Profile Instance Layer

The third layer of the architectural framework is the *federation profile instance* layer. While the first two layers of the architecture (the conceptual model and the federation profile) are

essentially schemas that define the structure of data objects, this layer is an actual data object or payload. It takes the form of an XML document that conforms to the XML schema of a specific federation profile. A profile instance is generated by an identity provider (IDP) that has firsthand knowledge of the attributes of a specific federated user or entity. The IDP builds it from data in a local attribute store, such as an LDAP directory or an ODBC database. The profile instance is intended for consumption by a service provider (SP) and is to be used for supporting identification, authentication, privilege management, auditing, and personalization. Implicit in the federation concept is that an SP may use the profile instance as it sees fit. It may choose to use all of the data elements within the profile instance, or it may use very few of the elements, ignoring certain data elements in a profile instance even though they may have been designated as mandatory by the federation profile for that federation. The goal of this layer is to allow an IDP to convey information about a federated user to an SP. How the SP chooses to use that information is outside the scope of the profile instance.

4.4 The SAML Assertion Layer

The fourth and final layer of the framework is the *SAML assertion* layer. This layer defines how a GFIPM metadata federation profile instance is encoded within and transported by an SAML assertion. An SAML assertion acts as a transport mechanism for a federation profile instance on its journey from an IDP to an SP. SAML assertions can carry attribute statements, which state facts about a user in the form of name/value pairs. The federation profile instance can be encoded within one or more SAML attributes inside an SAML attribute statement, which is itself sent from an IDP to an SP in an SAML assertion.

The specification of rules for encoding a federation profile instance in an SAML assertion has been a topic of investigation during the development of this framework. Several encoding strategies are possible, each with associated advantages and disadvantages. Vendor product support is a major consideration in the choice of an encoding strategy. Lessons learned regarding this issue were captured during the independent but related DOJ/DHS GFIPM Security Interoperability Demonstration Project, and several encoding recommendations have been made. A proposed standard for the encoding of metadata in SAML 2.0 assertions has been specified as part of GFIPM Metadata 1.0 package.

Table 2 summarizes each of the four layers.

Layer	Description
Conceptual Model	• Abstract conceptual model of information about a federation user or a federated entity • Provides consistent semantics and a formal basis for sharing information about users and other entities in a federation • Optional and over-inclusive, defines a superset of well-defined attributes pertinent to the GFIPM concept • Represented by a set of three GFIPM XML schemas, NIEM subset schemas, and a Microsoft Excel spreadsheet

Federation Profile	• A profile of the conceptual model that addresses the needs of a specific federation instance • Places subset and constraint rules on the abstract federated user and federated entity models as needed • Details of any specific federation profile are not an official part of the GFIPM metadata standard • Represented by a set of schemas that specify a subset of the schemas used to define the conceptual model
Federation Profile Instance	• XML instance that conforms to a specific federation profile • Encapsulates the metadata (data payload) for a specific authenticated federation user or federated entity conforming to the federation profile schema
SAML Assertion	• Acts as the transport mechanism for the XML instance between an identity provider and a service provider

Table 2: Layers of the GFIPM Metadata Framework

5. Feedback

As discussed in previous sections, the GFIPM metadata specification is expected to undergo several more iterations over the coming months and years. Comments and feedback from a broader set of reviewers are necessary to broaden the perspective beyond the requirements of the initial set of 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. Of special interest are comments in the area of the conceptual model of the federated user and associated metadata structure, definition, content, and usage. 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 and inclusion as part of the GSWG GFIPM work plan.

Appendix A: Metadata Sources

This appendix serves to acknowledge several contributing groups and projects for the specific metadata attributes that they have contributed to the GFIPM Metadata 1.0 data model. Most of the attributes in the GFIPM Metadata model have come from two sources: GFIPM Pilot Participants and GSWG Members. The metadata model has evolved through many iterations since 2004. The development process for GFIPM Metadata version 1.0 included a reconciliation effort between the GFIPM Metadata model and two recent metadata attribute projects in the justice community: the Department of Homeland Security (DHS) Project on Attribute-Based Access Control (ABAC)[2] and the Global Technical Privacy Task Team effort to define privacy-relevant attributes.[3] The results of each reconciliation effort are described here.

[2] See the technical report "Defining User Attributes for Authority-Based Access Control" by Waterman & Hammar.
[3] See the technical report "Implementing Privacy in Justice Information Sharing: A Technical Framework" and the web site http://www.privacywiki.org/.

DHS ABAC Project

The DHS ABAC initiative seeks to identify a set of base attributes that are critical for authorization decisions for current and future government information sharing systems, and also to identify the authoritative source of each critical attribute. The goal of the project's work is to identify attributes that can enable rule-based access control to be implemented based on the most current information available about a user at the time of an access attempt. The long-term vision of the project is for each attribute to be queried as needed from the attribute authority that is deemed to be authoritative for that attribute, thereby relieving applications of the need to constantly keep access control lists current. The overarching vision of the ABAC project is similar to GFIPM in the sense that both projects seek to relieve applications and resources of the burden of directly managing data about users.

The reconciliation effort between the GFIPM Metadata and the DHS ABAC Project work produced the following results. Many of the ABAC metadata attributes about users already existed within the GFIPM Metadata standard prior to this reconciliation process; however, there were several ABAC attributes that did not exist in the GFIPM Metadata standard. Table A.1 lists all of the ABAC attributes that are considered relevant to GFIPM but were not already included in the GFIPM Metadata standard. Along with each listed attribute is that attribute's current status as regards the GFIPM Metadata standard.

New ABAC Attribute	Current Status
Employment Type	Under Consideration for GFIPM Metadata 1.1
Job Designation	Under Consideration for GFIPM Metadata 1.1
Physical Location	Under Consideration for GFIPM Metadata 1.1
Location Type	Under Consideration for GFIPM Metadata 1.1
Management Level	Under Consideration for GFIPM Metadata 1.1
List of Direct Reports	Under Consideration for GFIPM Metadata 1.1
Rating/Reviewing Official	Under Consideration for GFIPM Metadata 1.1
Authorized Purpose	Under Consideration for GFIPM Metadata 1.1
Skills and Skill Levels	Under Consideration for GFIPM Metadata 1.1

Table A.1: Status of New ABAC Attributes in GFIPM Metadata

Global Technical Privacy Task Team

The Global Technical Privacy Task Team is a technical standards group that is working on the task of translating privacy and requirements into technical specifications and standards. It focuses on identification, specification, and addressing standards for privacy for Global. The scope for the tasks and deliverables of this task team covers the entire justice domain, including local, state, regional, tribal, and federal organizations. One of the responsibilities of this team is to identify a set of privacy-related metadata that apply to information sharing transactions within the law enforcement community.

The reconciliation effort between the GFIPM Metadata and the Global Technical Privacy Task Team work produced the following results. Most of the privacy metadata about users already existed within the GFIPM Metadata standard prior to this reconciliation process. Also, some of

the privacy-relevant user metadata not already captured within the GFIPM Metadata standard is actually metadata about the relationship between a user and the subject of a transaction, e.g. an attorney-client relationship. This type of relationship metadata falls outside the current boundaries of the GFIPM Metadata standard, because it pertains to a specific transaction and is not constant across transactions for a given user. After factoring out these two categories of privacy-relevant user metadata – items already found within the GFIPM Metadata standard and items that are not transaction-independent – there were very few new user metadata concepts that remained as candidates for inclusion in the GFIPM Metadata standard. Table A.2 lists all privacy attributes identified by the Technical Privacy Task Team's work that are considered relevant to GFIPM but were not already included in the GFIPM Metadata standard. Along with each listed attribute is that attribute's current status as regards the GFIPM Metadata standard.

New Privacy Attribute	**Current Status**
Level of Government	Included in GFIPM Metadata 1.0
Professional Licenses	Under Consideration for GFIPM Metadata 1.1
Employment Role	Under Consideration for GFIPM Metadata 1.1

Table A.2: Status of New Privacy Attributes in GFIPM Metadata