Trust Framework Provider Assessment Package

US ICAM LOA 1 V2

2011-11-08

This document comprises the Assessment Package submitted by the Open Identity Exchange Corporation (OIX) to the United States Office of Governmentwide Policy (OGP) per the process defined in the Trust Framework Provider Adoption Process (TFPAP) published on the http://www.idmanagement.gov/ website by the Identity, Credential, and Access Management (ICAM) Subcommittee of the Information Security and Identity Management Committee of the U.S. Federal CIO Council.

Section 3.1 of the TFPAP reads:

> *The process begins with an Applicant TFP (Applicant) submitting an Assessment Package to OGP, which then raises the submission to the ICAMSC. The Assessment Package must include the framework's trust specifications with respect to applicable NIST SP 800-63 LOA trust criteria listed in Appendix A, the framework's privacy specifications with respect to Section 3.3 privacy criteria, the Applicant's audit and re-certification processes, the Applicant's auditor qualifications, and evidence of the Applicant's organizational maturity. The Assessment Package must build the case that the Applicant's trust model and practices are comparable at the desired LOA. Applicants are not required to submit their assertions in any particular format, nor are they required to comply strictly with any particular trust criterion. Instead, the Applicant must demonstrate that its trust specifications meet or exceed the trust criteria in NIST SP 800-63. Failure to comply with any particular requirement is not fatal, since alternative mitigation strategies may satisfy trust criteria, especially at LOA 1 and LOA 2.*

Accordingly, this Assessment Package consists of the following sections:

[1] Terminology note: OIX uses the term "assessor" for the role TFPAP refers to as an "auditor".

Appendix F: Open Identity Trust Frameworks: An Introduction

1. OIX Background

The Open Identity Exchange Corporation (OIX) was established as a Washington State Non-Profit Corporation on 3 February 2010 in response to the expression of support memorialized in a set of Mirror Resolutions approved by the Board of Directors of the Information Card Foundation (ICF) on 15 January 2010 and the Board of Directors of the OpenID Foundation (OIDF) on 20 January 2010.

The founding Board of Directors of OIX includes Don Thibeau, Executive Director, OpenID Foundation; Ron Carpinella, VP Identity, Equifax; Eric Sachs, Product Manager for Google Security, Google; Andrew Nash, Senior Director of Information Risk Management, PayPal; Nico Popp, Vice President of Innovation, Verisign; and Peter Tibbett, Vice President of Technology and Innovation; Verizon.

The charter of OIX is to serve as an independent, neutral, international provider of certification trust frameworks conforming to the Open Identity Trust Frameworks model described in Appendix F. The first trust framework OIX intends to serve is the US ICAM LOA 1 V1 Trust Framework as defined in this Assessment Package.

1.1 OIX Parentage

Passage of the Mirror Resolutions supporting the establishment of OIX was the result of nine months of dialog, research, and planning among OIDF, ICF, and ICAM that began in April 2009. This dialog began when ICAM asked each foundation to consider how a public/private partnership could best provide open identity solutions that could serve all members of the public while still meeting the identity assurance and protection requirements of U.S. government websites. Feedback from OIDF, ICF, and other industry groups resulted in announcement of the Open Identity Solutions for Open Government initiative at the Gov 2.0 conference on 10 September 2009.

The OpenID Foundation is an Oregon Non-Profit Corporation established in June 2007 for the purpose of advancing the use of OpenID as an open, Internet-scale user-centric digital identity management solution. OIDF follows a community governance model where the majority of the members of the OIDF Board of Directors are elected by the OpenID community. As of the time of this application, the community members of the OIDF Board of Directors are:

- Brian Kissel (JanRain), Chair
- Nat Sakimura (NRI), Vice-Chair
- Chris Messina (Google), Secretary
- David Recordon (Facebook)
- Joseph Smarr (Google)
- Allen Tom (Yahoo!)
- Marc Frons (New York Times)
- Daniel Jacobson (NPR)
- John Bradley (Independent)
- Dick Hardt (Independent)
- Robert Harles (Sears)

The OIDF Board also includes one representative from each OIDF Sustaining Member. As of the time of this application, the OIDF Sustaining Members are:

- Booz Allen Hamilton
- Facebook
- Google
- IBM
- LexisNexis
- Microsoft
- PayPal
- Ping Identity
- Verisign
- Yahoo!

One of the primary purposes of OIDF is to maintain the integrity of the OpenID Community Process for development of the open standard OpenID specifications. The OpenID 2.0 Authentication protocol created using this process was ratified by the OpenID Foundation board on 5 December 2007. Per the Identity Scheme Adoption Process (ISAP), ICAM determined that OpenID 2.0 was of sufficient value to adopt as an ICAM identity scheme. ICAM published version 1.0.1 of the OpenID 2.0 Profile on 18 November 2009.

The Information Card Foundation is a Delaware Non-Profit Corporation established in March 2008 for the purpose of advancing the adoption of Information Cards as a universal user experience metaphor for digital identity transactions based on an underlying identity metasystem that incorporates different technologies and token formats. ICF follows the same community governance model as the OIDF where the majority of the members of the ICF Board of Directors are elected by the OpenID community. As of the time of this application, the community members of the ICF Board of Directors are:

- Paul Trevithick (Azigo), Chair
- Craig Burton (Burtonian)
- Kim Cameron (Microsoft)
- Pam Dingle (Ping Identity)
- Patrick Harding (Ping Identity)
- Andy Hodgkinson (Microsoft)
- Ben Laurie (Google)
- Axel Nennker (Deustche Telecom)
- Mary Ruddy (Meristic)

The OIDF Board also includes one representative from each OIDF Steering Member. As of the time of this application, the OIDF Steering Members are:

- Booz Allen Hamilton
- Equifax
- Deustche Telecom
- Google
- Microsoft
- Oracle
- PayPal
- Verizon

Biographies of all ICF board members are available on the Board of Directors web page.

The first technical protocol to fully support Information Cards is the IMI (Identity Metasystem Interoperability) 1.0 protocol published by the OASIS IMI Technical Committee. IMI Version 1.0 was approved as an OASIS Standard (the highest level of standardization available through OASIS) on 1 July 2009.

Per the Identity Scheme Adoption Process (ISAP), ICAM determined that IMI 1.0 was of sufficient value to adopt as an ICAM identity scheme. ICAM published version 1.0.1 of the Identity Metasystem Interoperability 1.0 Profile on 18 November 2009.

1.2 OIX Management and Administration

The Chairman of the OIX Board of Directors is Don Thibeau, who currently serves as the Executive Director of the OpenID Foundation. Mr. Thibeau joined the foundation at the beginning of 2009 to position the organization and its membership for long-term growth. Mr. Thibeau has a rich background in the data, identity, and social layers of both telephony and Web transactions. An information technology industry expert, Thibeau has had senior management positions with leading organizations including TransUnion, Reed Elsevier and LexisNexis. Thibeau is a frequent guest speaker and has testified before Congress on topics including data privacy and regulatory issues. He is a former Presidential appointee and White House liaison for the US Synthetic Fuels Corporation.

The Acting Executive Director of OIX is Drummond Reed, who currently serves as the Executive Director of the Information Card Foundation. Mr. Reed is a founding director of both ICF and OIDF, as well as the International Security, Trust, and Privacy Alliance (ISTPA), XDI.org, Identity Commons, and DataPortability.org. He also serves as co-chair of the OASIS XRI and XDI Technical Committees, and as a member of the OASIS IMI Technical Committee. In 2003 Mr. Reed received the Digital Identity Pioneer Award from Digital ID World for his work on XNS, the predecessor to XRI and XDI.

Legal counsel for OIX is K&L Gates, one of the world's most respected law firms. The firm has approximately 1,800 lawyers who practice in 35 offices located on three continents. K&L Gates represents leading global corporations, growth companies, and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. Scott David, a partner at K&L Gates is lead counsel for the OIX legal team at K&L Gates. The team includes

experienced representatives of various areas of the firm's practices relevant to the organization and operation of OIX, and the identity management services market that it is intended to support. Scott is co-chair of the Identity Commons Legal Working Group, and he heads the "Identity Law Common Definitions Project" of the American Bar Association's Business Section, Cyberspace Law Committee. Scott has practiced law for over 25 years. At Simpson Thacher and Bartlett he did legal work in the financial markets and in tax. Since the early 1990's he has provided legal advice to software, ecommerce, telecommunications, social networking, virtual-reality services and other new technology clients on issues involving online commerce; privacy and data security laws; online payment systems and tax administration systems; identity and information system structuring; intellectual property licensing; entity structuring; technology development and transfer; participation in standards setting organizations; and tax.

Operational administration for OIX ("OIX Administrator") is provided by Global Inventures, one of the premier alliance and certification management companies in the industry. Headquartered in the San Francisco Bay Area, Global Inventures was formed in 1992 and focused initially on providing diligence services to venture capital firms. The firm subsequently moved into building collaborative alliances between technology companies to seed and grow markets based on new technologies and industry solutions.

Today Global Inventures engagements represent more than 10,000 private and public sector entities around the world, including start-ups, tech heavyweights, academic institutions, and government bodies. More details on Global Inventures and its management team is available on the Global Inventures website at http://www.inventures.com/.

2. Overview of the OIX Trust Framework Provider Model

OIX was established to provide trust framework provider (TFP) services based on the Open Identity Trust Frameworks (OITF) model set forth in the white paper attached as Appendix F. This section is only a brief synopsis of this model; please see the white paper for more details.

The fundamental premise of the OITF model is that an open market design is the most efficient and effective way for market participants to satisfy the continuing identity assurance and data protection requirements of a particular trust community, and to promote the improvement of the services that those market participants offer.

In this case, the trust community is the U.S. government, as represented by ICAM and GSA, and the requirements are those defined in the TFPAP and the OpenID 2.0 and IMI 1.0 Profiles (collectively referred to as the "ICAM Trust Framework").

Under the open market model, OIX does not define its own native trust framework and then map that trust framework to ICAM's requirements. Instead, OIX takes the requirements specified in the ICAM Trust Framework as its starting point. OIX then manages an open market process to enable the best available identity management services to be matched with the trust framework needs. This process consists of the following overall steps:

2.1 Assessor Qualification

- OIX has accepted FICAM Privacy Guidance for Trust Framework Assessors and Auditors Version 1.0 as an assessment guide. The guide should be used by Assessors and Auditors when determining whether an Applicant Identity Provider intending to interact with Federal agency applications should be approved, and during re-assessment audits required for renewal of a certification. The full guide can be found on the Federal Identity, Credential and Access Management home page or by following this link: http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV.
- For each trust community OIX serves, OIX receives from the trust community (in this case, ICAM) a description of any requirements for specific parties (or parties that meet certain criteria) to act as Special Assessors. A Special Assessor has the qualifications necessary to verify the qualifications of other Assessors for the trust framework (that reflects the identity management service needs of that trust community) at specific levels of assurance (LOAs).
- To become a Registered Assessor for a specific trust framework, an Assessor must first be an OIX General Member. This requires submitting the OIX Membership Application Form (attached as Appendix C) and an executed copy of the OIX Membership Agreement (attached as Appendix D) to OIX. This legally binds the Assessor to the OIX Operating Rules as well as the rules of any trust framework for which the Assessor becomes a Registered Assessor.
- If the information is verified, OIX accepts the Assessor as an OIX General Member.
- Next the Assessor must submit to the Special Assessor for a selected trust framework and LOA the information required in the Assessor Application Requirements for that

trust framework and LOA. The OIX US ICAM LOA 1 V1 Assessor Application Requirements are attached as Appendix A.
- The Special Assessor then conducts an evaluation of the Assessor.
- Once the evaluation is successful, the Assessor submits to OIX the Assessor Specialty Member Addendum (Attachment B to the OIX Membership Application Form).
- OIX verifies the submitted information, including that the evaluation by the Special Assessor was successful.
- If the information is verified, OIX lists the Assessor as a Registered Assessor for the selected trust framework and LOA.

2.2 Identity Provider Qualification

This process is identical to that of Assessors described in section 2.1, except that an Identity Provider may choose from any Registered Assessor for the trust framework and LOA for which the Identity Provider desires to be certified.

- To become a Registered Identity Provider for a specific trust framework, an Identity Provider must first be an OIX General Member. This requires submitting the OIX Membership Application Form (attached as Appendix C) and an executed copy of the OIX Membership Agreement (attached as Appendix D) to OIX. This legally binds the Identity Provider to the OIX Operating Rules as well as the rules of any trust framework for which the Identity Provider becomes a Registered Identity Provider.
- If the information is verified, OIX accepts the Identity Provider as an OIX General Member.
- Next the Identity Provider must submit to a Registered Assessor for a selected trust framework and LOA the information required in the Identity Provider Application Requirements for that trust framework and LOA. The OIX US ICAM LOA 1 V1 Identity Provider Application Requirements are attached as Appendix B.
- The Registered Assessor then conducts an evaluation of the Identity Provider.
- Once the evaluation is successful, the Identity Provider submits to OIX the Identity Provider Specialty Member Addendum (Attachment B to the OIX Membership Application Form).
- OIX verifies the submitted information, including that the evaluation by the Registered Assessor was successful.
- If the information is verified, OIX lists the Identity Provider as a Registered Identity Provider for the selected trust framework and LOA.

Because the identity management services sector is evolving rapidly, OIX can best serve trust communities and other market participants by proceeding incrementally to develop and deploy successful trust frameworks, in discrete steps that allow participants to engage in the market in a measured fashion to allow familiarity, confidence and trust to build among all parties.

In furtherance of this goal, this first Assessment Package specifies OIX certification processes for the ICAM Trust Framework at LOA 1. Since the OITF model also provides means for trust framework specifications to be versioned as they evolve, these

specifications will be referred to as **US ICAM LOA 1 V3**. Should OIX need to submit a revised Assessment Packages for LOA 1 in the future, it will have new version number.

OIX also intends to submit Assessment Packages for LOA 2 and LOA 3 once it has implemented LOA 1 V1.

Table 1: OIX Organizational Maturity

The following requirements are specified in section 3.3 of the TFPAP.

#	Requirement	Applicant Response
a	Applicant legal status	OIX is an incorporated Washington State non-profit corporation.
b	Appropriate authorization to operate;	The purposes of OIX stated in its articles support its function as a neutral, non-profit trust framework provider as defined in the TFPAP.
c	Legal authority to commit the Applicant to conducting assessments and certifying Identify Providers on behalf of the Federal government;	OIX is a Washington State non-profit corporation duly formed for purposes that enable it to serve as a neutral, non-profit trust framework provider for trust frameworks defined by governments, industry associations, academic institutions, and other trust communities. Under the OIX Bylaws, the OIX Executive Director as President of the corporation is authorized to commit OIX to engage in activities that include conducting assessments and certifying identity providers on behalf of the Federal government.
d	Financial capacity to manage the risks associated with conducting assessments and certifying Identify Providers on behalf of the Federal government;	OIX is funded with separate grants from the OpenID Foundation and Information Card Foundation, and fees from its constituent members. By implementing the open identity assurance market model described in the Open Identity Trust Frameworks white paper attached as Appendix A, OIX enables the market to spread the risks among qualified assessors, identity providers, and relying parties that participate in the market mechanism enabled by OIX. OIX will carry D&O insurance with a minimum coverage of $1,000,000 and E&O insurance with a minimum coverage of $2,000,000. OIX Rules will establish criteria for requiring Assessors to carry E&O insurance commensurate with the level of risk established by the trust framework and level of assurance for which they are registered to perform an assessment.
e	Understanding of, and compliance with any legal requirements incumbent on the Applicant in connection to conducting assessments and certifying Identify Providers on behalf of the Federal government;	A key consideration in the formation of OIX was to identify a legal structure that would simplify the operation, administration, and legal analysis for an open market in identity services. The concept is that a simple organization that enables a simple open market through information sharing can be engaged with, simply, by Trust Communities that require identity management services. Simpler legal structures allow for simpler contracts, which helps people understand legal issues. This, in turn, reduces uncertainty and engenders the identification and adoption of common customs, approaches, and standards in the identity management industry. OIX will fulfill its mission of providing a neutral, open market registration system for participants in the identity-related services industry by maintaining a broadly accessible Listing Service detailing Trust Framework needs and Identity Provider, Assessor and other identity management related services offerings. The intention of the Listing Service is to disseminate information about identity management services and needs and to thereby enable ready access to helpful market information by both providers and

		users of identity services; the emergence of "best practices," evolving interdisciplinary standards, and broad interoperability to the benefit of Trust Communities and data subjects as well as other market participants. The information exchange mechanism used by OIX to support this market is intentionally flexibly structured in order to permit it to be responsive to the inevitable changes that will take place in this industry. This information exchange structure also has the benefit of being less legally complex. The inflow of Registration Information from identity management industry participants is managed through the membership application process and specifically the OIX Membership Application/Member Agreement structure (Appendices C and D). This structure is based on well developed legal structures characteristic of other similar non-profit associations and entities that offer certification structures for other markets (such as NASD/FINRA). Information outflow, i.e., access to the OIX information by Members and the public, is managed through a relatively standard Terms of Use document, like that used on many websites. Together, the legal documents form the rules for the information flows that support the open market mechanism enabled by OIX operations. In other respects, OIX bears some resemblance to industry standard-setting initiatives (and, indeed, enabling open standards is one of the goals of OIX), and so the legal issues associated with those efforts will also be relevant in the analysis of OIX organization and operation. Those issues are relatively well developed given the prevalence of such initiatives. Finally, OIX intends to file an application with the U.S. Internal Revenue Service for recognition of exemption as a 501(c)(6) "trade association" organization. Qualification for that status carries certain requirements that, rather than being viewed as limitations on OIX activity, offer a familiar structure that has been used to help standardize and normalize myriad industries to the benefit of providers and users of products and services, and is characterized by relatively settled law. Again, this will help to reduce the overall complexity of the legal structuring of OIX by resorting to more established types of structures to accomplish OIX goals. In addition to the legal requirements associated with OIX operations described above, there are other laws that will be relevant to OIX operations. Even though OIX will never itself handle any personal information or other identity related information, the Assessors, Identity Providers, Relying Parties, Trust Frameworks, and others involved in the open identity services market will handle such information, and are therefore subject to a variety of laws that will affect the manner in which they design and implement their respective identity management services. OIX is designed specifically to address this situation in a way that helps all participants in the market, particularly trust frameworks. As new trust frameworks move into the market to pursue identity management services from identity providers, they will ask for these

		services to be responsive to an increasing range of laws, regulations, industry practices, customs and myriad other variables. An open market approach can "scale" to accommodate the requirements for any size trust framework, with any number of variables. The federal government is very complex, as are its data needs. In the U.S., different types of identity-related data are subject to entirely different, sometimes conflicting, laws and rules. Under U.S. federal law the "sector specific" approach to regulation has resulted in different laws being developed in relative isolation from one another to address the issues of data security and privacy in that particular sector. For example, the following federal laws potentially apply to impose requirements on the use and handling of data in the following areas, each of which could be relevant to a potential OIX Registered Trust Framework, and some of which will be relevant to the ICAM Trust Framework. **Financial** (Gramm Leach Bliley Act; Right to Financial Privacy Act of 1978;), **Bank Records** (Bank Secrecy Act) **Census Data** (Census Confidentiality Statute) **Tax information** (26 CFR Parts 301 and 602) **Genetic Information** (Genetic Information Nondiscrimination Act of 2008) **Medical/Health** (Health Insurance Portability and Accountability Act of 1996 (HIPAA)(as amended by HITECH Act under ARRA), **Consumer/Credit Reports** (Fair Credit Reporting Act (FCRA) and FACT) **Education Records** (Family Educational Rights and Privacy Act) **Phone Related Information** ("CPNI" under Federal Communications Act, and "CPRI" under Telephone Records and Privacy Protection Act of 2006) **Cable TV Records** (Cable Communications Policy Act of 1984) **Health Records Breach Notices** (American Recovery and Reinvestment Act of 2009) **Data Relating to Children** (Children's Online Privacy Protection Act) **Government Data Matching** (Computer Matching and Privacy Protection Act of 1988) **Driver records** (Driver's Privacy Protection Act of 1994) **Video Rental Records** (Video Privacy Protection Act of 1988) **SSN display by states** (42 USC 405(c)(2)(C)(vi)) **Duplicative collection of information by federal agencies** (Paperwork Reduction Act of 1980). **Federal Records with personal information** (Privacy Act of

		1974). **Research data on individuals** (Public Health Service Act) This is just a small subpart of the laws that apply in the U.S. to identity related data. In addition to the federal law, the 50 states within the U.S. each have a variety of breach notice, data security, SSN handling, and other personal information (PI) transfer, data disposal and other sector-specific laws that may apply to the data that is used and relied upon in the course of providing identity management services to a Trust Framework. Because OIX does not need to handle any of the listed types of data in order to enable the market (it handles information *about* the services, not the data that is used *by* the services), it should not be subject to any such data laws. Its agreements with its Members are structured consistently with this approach. These laws are, however, very relevant to how OIX structures its Listing Service. The various laws have commonalities of process, definitions and other attributes that can be identified in an open market. Once these commonalities are identified, identity management services can be configured to achieve the maximum efficiency (and for identity providers, maximum market expansion) by managing identity data in a way that takes maximum advantage of the presence of common requirements, i.e., by standardization of technology and policies associated with those commonalities. In summary, data security, privacy and other laws and rules associated with identity information inform OIX processes, but the structure of OIX enables OIX to avoid the need to configure its operations to address all such laws (which would be a very expensive proposition were it to be undertaken). This permits the OIX model to scale with the requirements of the participants in the market.
f	Scope and extent of implemented security controls (e.g., access control, confidentiality of Identity Provider information);	OIX will not handle any personal information or other data of consumers that is the subject of various regulation (and much legal uncertainty). Instead, the main activity of OIX will be to receive and make available Registration Information from market participants. Registration Information will include information from Trust Frameworks about their needs, and information from Identity Providers, about their capabilities. Registration Information also includes information about Assessor capabilities. All of this information is being shared among businesses, governmental entities, academic entities and other providers and users of identity management services. OIX Registration Information is about the services in the identity management market, not about the data hosted by the participants in that market The legal issues associated with the movement of the Registration Information through the OIX system involves relatively straight-forward B2B commercial terms (for example it is documented through relatively standard copyright, trademark and other intellectual property licensing provisions). To further reduce complexity and assure transparency in the market, all Registration Information supplied directly to OIX is

		required by OIX Rules to be non-confidential, reducing the legal issues and administration associated with maintaining confidentiality. It is recognized that there will be situations in which confidential information may need to be handled, but those are assumed to be the exception in this open market. While Registration Information that is provided to OIX is typically required to be nonconfidential, it is still possible that confidential information could be shared among Trust Communities, Identity Providers, Assessors, and other parties involved in the evaluation and provision of identity management services. Where such confidential or other protected information (such as PII) is being held and transferred by and among these parties, policies and agreements among the parties will address the confidentiality issues. The fact that OIX will not handle any personal information (other than contact information of the individual representatives of the companies that register with OIX), and will not maintain any confidential information significantly reduces the security burden of OIX. The primary focus of OIX security systems will be to maintain standard controls associated with securing its website, information systems, and communications from impersonation, misappropriation, or malicious attack. OIX will use both conventional and extended validation certification SSL certificates for its website, and use SMIME or equivalent encrypted email when conducting confidential electronic communications requiring authentication and non-repudiability.
g	Documentation of policies and procedures;	OIX administration will follow the certification administration policies and procedures developed in 15 years of industry practice by OIX Administrator Global Inventures. These are currently being developed to the specific requirements of the TFPAP and the US ICAM LOA 1 V1 trust framework as defined in this Assessment Package. Global Inventures is available for direct interview regarding compliance with this requirement; see Appendix E for more information.
h	Proof that Applicant practices are consistent with documented policies and procedures (e.g., via independent auditor reports, if required by LOA requirements);	OIX Administrator Global Inventures is available for direct interview regarding compliance with this requirement; see Appendix E for more information.

Table 2: OIX Review of Member Organizational Maturity

Requirement (a) is specified in section 3.3 of the TFPAP. Requirements (a1) through (a8) are specified by Applicant.

#	Requirement	Applicant Response
a	Determination of whether the Applicant sufficiently reviews member identity provider *bona fides* to ensure member identity provider organizational maturity, legitimacy, stability, and reputation.	Applicant's process for verifying the *bona fides* of a member identity provider is a mirror of the process ICAM specifies in Table 1 to verify the *bona fides* of Applicant. Applicant's requirements are stated in the Requirements column of rows (a1) through (a8). Applicant's processes for assessing conformance with each requirement are stated in this column.
a1	Verify IdP legal status	Registered Assessor must verify IdP's articles of incorporation and current filing status.
a2	Verify IdP has appropriate authorization to operate as an identity provider;	Registered Assessor must verify IdP's bylaws and presence of any identified licenses.
a3	Verify IdP has legal authority to commit the IdP to serve as an identity provider on behalf of the Federal government;	Registered Assessor must verify that an officer or director of IdP has duly authorized such activity.
a4	Verify IdP has the financial capacity to manage the risks associated with serving as an identity provider on behalf of the Federal government;	Registered Assessor must review IdP's financial statements and verify that IdP has adequate insurance policies and limits, including Errors and Omissions coverage of at least $2,000,000, Directors and Offices coverage, and any other applicable policies.
a5	Verify IdP has understanding of, and compliance with any legal requirements incumbent on the IdP in connection to serving as an identity provider on behalf of the Federal government;	IdP is required to submit a written statement confirming the OIX Membership requirement of compliance with applicable law including compliance with the legal requirements in Table 1, row e, and with any other legal requirements that may be in effect for the jurisdiction in which the IdP operates. Registered Assessor must interview IdP regarding its understanding of these requirements and the policies and procedures it uses to comply with these requirements.
a6	Verify the scope and extent of IdP's implemented security controls (e.g., access control, confidentiality of user information, facility security);	Registered Assessor must (i) review IdP's security policies, (ii) review IdP's security certifications, e.g., ISO/IEC 27002, (iii) ask about reported security breaches.
a7	Verify IdP has documentation of policies and procedures;	Registered Assessor must review copies of IdP's policies and procedures and interview IdP regarding implementation of these policies and procedures.
a8	Review proof that IdP practices are consistent with documented policies and procedures (e.g., via independent auditor reports, if required by LOA requirements);	Registered Assessor must review independent auditor reports if available (and deemed relevant to assessing compliance at LOA 1).

Table 3: OIX US ICAM Privacy Requirements for Members

Requirements in the following table are specified in section 3.3 of the TFPAP.

#	Requirement	Applicant Response
a	**Opt In** – Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of individual attributes for each transaction.	IdP must provide Registered Assessor with documentation of how it conforms to this requirement and give specific examples. Registered Assessor must verify that the documented IdP practices conform to this requirement.
b	**Minimalism** – Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile. RP Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002.	IdP must provide Registered Assessor with documentation of how it conforms to this requirement and give specific examples. *NOTE: The last sentence of this requirement is not applicable to IdPs.* Registered Assessor must verify that the documented IdP practices conform to this requirement.
c	**Activity Tracking** – Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication. RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002.	IdP must provide Registered Assessor with documentation of how it conforms to this requirement. *NOTE: The last sentence of this requirement is not applicable to IdPs.* Registered Assessor must verify that the documented IdP practices conform to this requirement.
d	**Adequate Notice** – Identity Provider must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process.	IdP must provide Registered Assessor with documentation of how it conforms to this requirement and give specific examples. Registered Assessor must verify that the documented IdP practices conform to this requirement.
e	**Non Compulsory** – As an alternative to 3rd-party identity providers, agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service.	*OIX believes this requirement applies solely to RPs and is not applicable to assessment of IdPs.*

f	**Termination** – In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.	IdP must provide Registered Assessor with written documentation of its policies and practices for how it will continue to protect any sensitive data including PII if IdP ceases to provide this service. Acceptable policies are that upon cessation of service: 1) IdP will destroy all sensitive data including PII, or 2) If IdP retains such data for lawful purposes, IdP will continue to provide this data equal or greater protection than if IdP was still providing the service. Registered Assessor must verify that the documented IdP policies and practices conform to the criteria above.

Table 4: OIX Assessor Qualifications

The following requirements are specified in section 3.3 of the TFPAP.

#	Requirement	Applicant Response
a	Demonstrate competence in the field of compliance audits;	Assessor must provide written evidence of the assessor's qualifications and experience in the field of compliance audit, including a resume, a list of compliance audits performed in the past two years, and a list of at least three references. Special Assessor must review the written evidence, interview the Assessor, and check the provided references.
b	Be thoroughly familiar with all requirements that the Applicant imposes on member identity providers;	Assessor must demonstrate thorough knowledge of: (i) OIX Operating Rules as stated in the OIX Membership Application and the OIX Membership Agreement, (ii) The TFPAP, the ICAM OpenID 2.0 Profile and/or the ICAM IMI 1.0 Profile (whichever is relevant to the assessments this Assessor will be conducting), (iii) Security and identity assurance standards supporting the TFPAP, in particular NIST Special Publication 800-63. Special Assessor must interview Assessor to verify this knowledge.
c	Perform such audits as a regular ongoing business activity;	Assessor must provide written evidence that it performs such audits as a regular ongoing business activity, including tax filings showing a relevant industry code, financial statements showing a majority of revenue from compliance auditing, and a list of compliance audits performed in the past two years together with contact information for verification. Special Assessor must review the written evidence and verify that the audits were performed to the satisfaction of the relevant authority.
d	Be Certified Information System Auditors (CISA) and IT security specialist – or equivalent.	Assessor must provide either: a) CISA credentials, b) alternate credentials equivalent to CISA, or c) written documentation and at least three references that substantiate that Assessor's qualifications equal or exceed those required for certification by CISA. Special Assessor must review the evidence and verify either that: a) the CISA credentials are valid, b) the alternate credentials are valid and reasonably equivalent to CISA certification, or c) that the written documentation and supplied references support a clear and convincing conclusion that the Assessor's qualifications equal or exceed those required for CISA certification.

Table 5: OIX Process to Certify Members

The following requirements are specified in section 3.3 of the TFPAP.

#	Requirement	Applicant Response
a	Applicant's processes to audit (assess) members	The OIX certification assessment process is comprised of the following steps: 1) IdP must complete and submit the OIX Membership Application Form and OIX Membership Agreement to the OIX Administrator. This legally binds the IdP to the OIX Operating Rules as well as the rules of any trust framework for which the IdP becomes a Registered IdP. 2) OIX must verify the submitted information and, if verified, accept the IdP as an OIX General Member. 3) IdP must submit the information specified by the OIX US ICAM LOA 1 V1 Identity Provider Application Requirements (Appendix B) to a Registered Assessor (an Assessor qualified by the requirements in Table 2). In each response, the IdP must provide a description of how it meets or exceeds the requirement by either: a) *direct conformance*—practices and procedures that conform to the requirement as written, or b) *comparability*—practices and procedures that achieve equivalent or superior results to direct conformance. Each description must include references to any supporting materials that will be required by the Registered Assessor to verify compliance. If such materials are confidential and cannot be publicly disclosed, they must be clearly marked as such (disclosure will be limited to the Registered Assessor). 4) Registered Assessor must complete an evaluation of the IdP on every requirement specified by the OIX US ICAM LOA 1 V1 Identity Provider Application Requirements (Appendix B). 5) If the response to any requirement is found to be deficient, Registered Assessor must notify the IdP and the IdP may correct such deficiencies and submit documentation of such revisions to the Registered Assessor. 6) If all responses are found to meet the requirements, Registered Assessor must notify the OIX Administrator that the evaluation was successful. 7) IdP must submit the Identity Management Services Provider Specialty Member Addendum of the OIX Membership Application Form to the OIX Administrator. 8) The OIX Administrator must verify the submitted information. 9) If verified, the OIX Administrator must list the IdP as an Registered IdP for the US ICAM LOA 1 V1 Trust Framework and notify GSA as specified in processes to be mutually agreed between OIX and GSA.

Table 6: OIX Process to Recertify Members

Requirement (a) below is specified in section 3.3 of the TFPAP. Requirement (b) is specified by OIX.

	Requirement	Applicant Response
a	Applicant's ongoing processes to re-certify members	The OIX recertification assessment process is comprised of the following steps: 1) Within one year after becoming a Registered IdP as defined in Table 5, and every year thereafter, OR after any material change in IdPs business practices, Registered IdP must complete and submit the information required by the US ICAM LOA 1 Identity Provider Application Requirements (Appendix B) to a Registered Assessor (an Assessor qualified by the requirements in Table 2). If the IdP is using the same Registered Assessor as its previous assessment, the IdP only needs to submit information that is new since the previous assessment. 2) Within 15 days of receipt of this new information, Registered Assessor must complete a reassessment of the IdP on every affected requirement in the US ICAM LOA 1 Identity Provider Application Requirements (Appendix B). 3) If the response to any affected requirement is found to be deficient, Registered Assessor must notify the IdP and the OIX Administrator by the end of the 15 day period. 4) The IdP must correct such deficiencies and submit documentation of the revision to the Registered Assessor within 30 days. 5) The Registered Assessor must complete reassessment of the revisions within 15 days and notify the OIX Administrator of the results. 6) If any new information is found not to meet the requirements, the OIX Administrator must notify all parties including GSA, publish a notice of decertification on the OIX public website, and decertify the IdP. 7) If all new information is found to meet the requirements, the OIX Administrator must notify all parties and renew the IdP's registration as a Registered Identity Provider for the US ICAM LOA 1 V1 Trust Framework.

Table 7: US ICAM LOA 1 V1 Trust Criteria

The requirements in the tables in this section are from TFPAP Appendix A. The Applicant Response column indicates what the IdP must show the Registered Assessor in Table 5 step 3 or Table 6 step 1 order to prove it meets the requirement.

Table 7A: Registration and Issuance

Assurance Level 1 Trust Criteria	Applicant Response
1. A trusted relationship always exists between the RA and Identity Provider.	IdP must show mechanisms and policies are in place to ensure each party and its obligations are known to the other.
2. Sensitive data collected during the registration stage must be protected at all times (e.g. transmission and storage) to ensure its security and privacy.	IdP must show it sufficiently protects all sensitive data including PII (as defined by the Federal Government; see TFPAP Appendix C) obtained during registration as may be specified in NIST 800-63 or equivalent.
3. Resist token issuance disclosure threat.	IdP must show it issues tokens in a manner that protects confidentiality of information as may be specified in NIST 800-63 or equivalent.
4. Resist token issuance tampering threat.	IdP must show it establishes a procedure that allows the Subscriber to authenticate the CSP as the source of any token and credential data that he or she may receive as may be specified in NIST 800-63 or equivalent.
5. Resist unauthorized token issuance threat.	IdP must show it has established procedures to ensure that the individual who receives the token is the same individual who participated in the registration procedure as may be specified in NIST 800-63 or equivalent.
6. Some effort should be made to uniquely identify and track applications.	("Applications" means "requests for token".) IdP must show it has reasonable means to ensure that the same party acts throughout the registration, and token and credential issuance processes as may be specified in NIST 800-63 or equivalent.

Table 7B: Tokens

Assurance Level 1 Trust Criteria	Applicant Response
1. Resist token duplication threat.	IdP must show it protects against a Subscriber's token being copied with or without his or her knowledge (e.g., use tokens that are hard to copy) as may be specified in NIST 800-63 or equivalent.
2. Resist social engineering threat.	IdP must show it protects, as may be specified in NIST 800-63 or equivalent, against an Attacker establishing a level of trust with a Subscriber in order to convince the Subscriber to reveal his or her token or token secret.
3. For memorized secret tokens, pre-registered knowledge tokens, look-up secret tokens, and out of band tokens, the probability that an Attacker can guess a valid authenticator, over the lifetime of the token, must be less than 2^{-10} (1 in 1024).	IdP must show that the maximum probability that, over the life of the password, an Attacker with no *a priori* knowledge of the password will succeed in an in-band password guessing attack is lower than 1 in 1024. See NIST SP 800-63 Appendix A for complete discussion.

Table 7C: Token and Credential Management

Assurance Level 1 Trust Criteria	Applicant Response
1. Files of shared secrets used by Verifiers shall be protected by discretionary access controls that limit access to administrators and only to those applications that require access. Such shared secret files shall not contain the plaintext passwords.	IdP must show that it sufficiently protects shared secrets such as passwords as may be specified in NIST 800-63 or equivalent.
2. Long term token secrets should not be shared with other parties unless absolutely necessary.	IdP must show that any secret (e.g., password, PIN, key) involved in authentication is not disclosed to third parties by verifier or CSP, unless absolutely necessary.

Table 7D: Authentication Process

Assurance Level 1 Authentication Process Trust Criteria	Applicant Response
1. Resist online guessing threat.	IdP must show, as may be specified in NIST 800-63 or equivalent, that it protects against an Attacker performing repeated logon trials by guessing possible values of the token authenticator.
2. Resist replay threat.	IdP must show, as may be specified in NIST 800-63 or equivalent, that it protects against an Attacker being able to replay previously captured messages (between a legitimate Claimant and a Verifier) to authenticate as that Claimant to the Verifier.
3. Successful authentication requires that the Claimant shall prove, through a secure authentication protocol, that he or she controls the token.	IdP must show that it ensures that the Claimant (person being authenticated) actually possesses the token as may be specified in NIST 800-63 or equivalent.
4. Plaintext passwords or secrets shall not be transmitted across a network.	IdP must show that it does not transmit passwords or secrets in plaintext across an open communications medium, such as the Internet, used to transport messages between the Claimant and other parties.

Table 7E: Assertions

Assurance Level 1 Assertions Trust Criteria	Applicant Response
1. Use an ICAM adopted authentication scheme.	IdP must show that it uses one or more of the ICAM adopted authentication schemes defined for this assurance level.

Appendix A: US ICAM LOA 1 V1 Assessor Application Requirements

An Assessor is required to submit to a Special Assessor all of the information required for the Special Assessor to verify that the Assessor meets the requirements specified in:

1. Table 4: OIX Assessor Qualifications

Appendix B: US ICAM LOA 1 V1 Identity Provider Application Requirements

An Identity Provider is required to submit to a Registered Assessor all of the information required for the Registered Assessor to verify that the Identity Provider meets the requirements specified in:

1. Table 2: OIX Review of Member Organizational Maturity
2. Table 3: OIX US ICAM Privacy Requirements
3. Table 7: US ICAM LOA 1 V1 Trust Criteria

Appendix C: OIX Membership Application Form

This document is attached to the Assessment Package with the filename:

oix-tfp-pkg-2010-02-11-appendix-c-mem-app-form

Addendum 2010-03-03: The final version of this document is now available on the OIX website at:

http://www.openidentityexchange.org/sites/default/files/oix-membership-application-form-2010-02-26.pdf

The current version will be maintained at:

http://www.openidentityexchange.org/membership-documents

Appendix D: OIX Membership Agreement

This document is attached to the Assessment Package with the filename:

oix-tfp-pkg-2010-02-11-appendix-d-mem-agreement

Addendum 2010-03-03: The final version of this document is now available on the OIX website at:

http://www.openidentityexchange.org/sites/default/files/oix-membership-agreement-2010-02-26.pdf

The current version will be maintained at:

http://www.openidentityexchange.org/membership-documents

Appendix E: Letter from Global Inventures, OIX Administrator

This document is attached to the Assessment Package with the filename:

oix-tfp-pkg-2010-02-11-appendix-e-global-inventures

Addendum 2010-03-03: This letter summarized the qualifications of Global Inventures to serve as OIX Administrator. For current information about Global Inventures, please visit their website at http://www.inventures.com/.

Appendix F: Open Identity Trust Framework Model White Paper

This document is attached to the Assessment Package with the filename:

oix-tfp-pkg-2010-02-11-appendix-f-oitf-white-paper

Addendum 2010-03-03: The final version of this document is now available on the OIX website at:

http://www.openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf

The current version will be maintained at:

http://www.openidentityexchange.org/white-papers