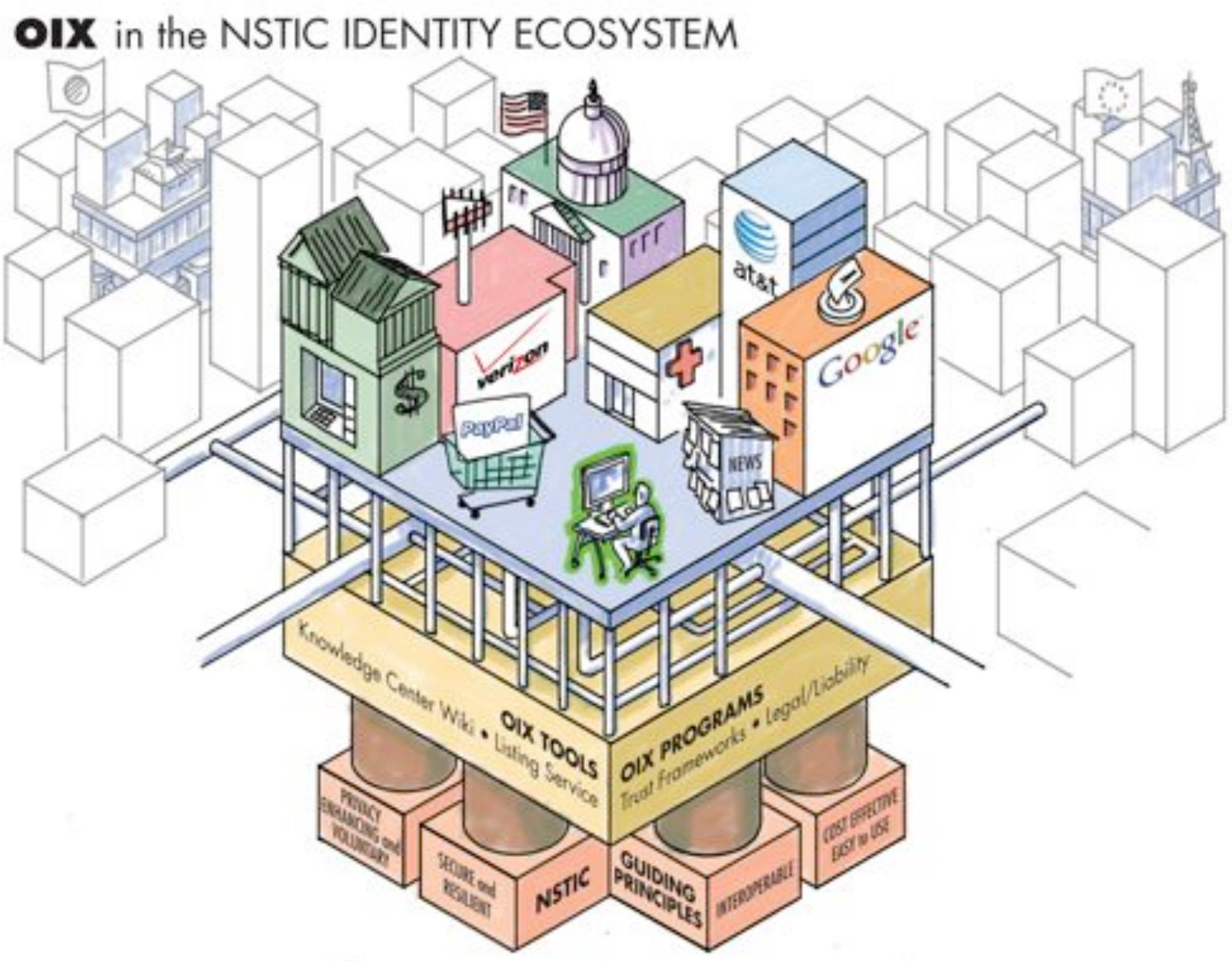
OIX OPEN IDENTITY EXCHANGE

# Open Identity Exchange (OIX) Response to:

## "Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace"

Notice of Inquiry
National Institute of Standards and Technology
[Docket No. 110524296-1289-02]



This is the response to the Notice of Inquiry entitled “Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace,” issued by The Department of Commerce and the National Institute of Standards and Technology (NIST) under docket no. 110524296-1289-02 (the “Governance NOI”) prepared by The Open Identity Exchange (OIX) for consideration by the Department of Commerce/NIST.

General Notes regarding the OIX Governance NOI response:

While the OIX board membership has had the opportunity to briefly review this draft, this document reflects the proposals and positions of only OIX in its role as a not-for-profit corporation formed to support the development of Trust Frameworks as a pathway to deploying comprehensive, integrated stakeholder solutions in emerging data/identity markets, and other related activities, and should not be taken to present the positions, proposals or policies of the individual member companies or their representatives.

In addition, this material is not intended to present legal advice. Individuals and commercial and governmental entities should consult with their respective legal and other advisers with respect to the implications of pursuing any of the strategies described herein, and before implementing any of the proposals presented herein.

# TABLE OF CONTENTS

# ***Introduction***

## EXECUTIVE SUMMARY

The NSTIC seeks to create what it calls the "Identity Ecosystem Framework;" that is, a set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that structure the Identity Ecosystem. To achieve that goal it calls for the creation of a private sector-led Steering Group to administer the process for development of the requisite policy and standards, and to ensure that accreditation authorities validate participants' adherence to the requirements of the Identity Ecosystem Framework.

The NSTIC emphasis on private-sector leadership is entirely consistent with the OIX efforts to support a community and marketplace of private-sector-led Trust Framework initiatives that help develop data/identity standards for various groups of stakeholders.

Thus, in addition to responding to the specific questions identified in the NOI, OIX has designed this response to:

- set forth its vision for the process by which the Identity Ecosystem Framework, and its component Trust Frameworks can best be developed;
- suggest an approach for the governance structure of the NSTIC Steering Group; and
- invite the National Program Office charged with achieving the goals of the Strategy, and the Steering Group it seeks to establish, to join with other stakeholder groups to avail themselves of OIX programs and tools to help to integrate the related "legal standards" setting processes.

The OIX vision for the Trust Framework development process is referred to as the "Participation Governance Model." It proposes the coordinated use of three pathways through which stakeholders can participate: i.e., via the Steering Group, the various Trust Framework development communities, and the online use of free, open source tools on the OIX website. Implementation of the Participation Governance Model is intended to support a market in standardized (and customized) data/identity products and services.

OIX believes that, by providing multiple pathways to stakeholder participation, the Participation Governance Model, and the technical and legal standard setting efforts it supports, will provide an effective form of industry self-regulation, and will clearly demonstrate that government action (such as legislation, regulation or new enforcement initiatives) is not necessary to achieve the NSTIC goals.

Additionally, a key goal of this response to the NOI is to make clear that OIX stands ready to support the Steering Group and the identity community generally as one of the key enablers of the Participation Governance Model.

## METHOD OF DEVELOPMENT

This NOI response is presented in two parts.

*Part 1* introduces a governance proposal that supports NSTIC called the "Participation Governance Model" that is presented through 8 diagrams and accompanying notes. The visual narrative describes how the NSTIC end-state called the "Identity Ecosystem Framework" can be supported through use of OIX programs and tools. Starting with the Identity Ecosystem diagram from the NSTIC document, it builds the diagram step by step to describe how the Steering Group, private sector Trust Framework initiatives, stakeholders, and the U.S. and other governments can coordinate their respective rule setting activities aided by OIX programs and tools.

*Part 2* sets forth the OIX responses to the four sets of questions raised in the NOI. These questions are grouped under the following general categories set forth in the NOI: Steering Group structure, Steering Group initiation, stakeholder participation and international issues. The OIX response to these questions is meant to be supplemental to the OIX vision outlined in Part 1's Participation Governance Model.

Additional exhibits relate to materials associated with Parts 1 and 2, and also present a discussion draft of a Steering Group Charter for consideration by interested parties This draft is a redlined version of the governance structure for the Smart Grid Interoperability Panel, which has been changed to reflect revisions appropriate for use of this structure for the identity Steering Group. While the governance structure for the Smart Grid Interoperability Panel was designed for a different industry (electricity versus data/identity) and on a different scale (U.S. versus international), it nonetheless provides a starting point for governance of an organization that, like the proposed Steering Group, is faced with issues of multi-stakeholderism in a networked market. Using this existing charter as a starting point may also help to expedite initiation of the Steering Group.

# KEY THEMES

What is the Participation Governance Model?

The Participation Governance Model is a multi-organization collaboration structure currently being applied by OIX, a non-profit organization the mission of which is to serve all data/identity market stakeholders by providing them with tools and programs through which they can have a "voice" in the creation of the rules that guide their behavior online. That "voice" is enabled through different channels including rule setting, policymaking and market mechanisms.

The model informs the overall structure of a "crowd sourced," self-regulatory virtual organization where the policies and rules are the subject of standardization by the same parties to which they will apply. This form of "self regulatory organization" incorporates and facilitates Internet scale, multi-jurisdictional application, legal subject matter, and provides stakeholders with access to processes that can help standards to better reflect their current needs including needs associated with the sometimes-sensitive issues of rule setting and standardization relating to those aspects of these systems with which individuals interact. The diagrams that follow will illustrate the form of this virtual organization.

The Participation Governance Model is at the heart of the Open Identity Exchange vision for private sector leadership in supporting Trust Framework development as an avenue toward standardization of "Tools and Rules" for data/identity markets. This approach is consistent with NSTIC, and is also intended to provide a flexible and extensible structure through which other non-U.S. and various sector-specific data/identity initiatives can effectively interact, collaborate and leverage their respective development resources to save costs and foster interoperability and innovation in the data/identity sector to best address their quickly-evolving needs.

The ultimate intention of the model is to support the coordinated movement of communities, markets and governance structures online. Part of that effort requires the building of Trust Online, including reliable, predictable identity assurance and related systems at Internet scale. Trust Frameworks are the legal/policy specifications that will establish the "rules standards" that will help make these systems reliable. Rules development is the subject of the standards development in the virtual organization described by the diagrams.

The Participation Governance Model is about building efficacy, efficiency, stakeholder control, reliability, predictability interoperability and "trust" into the architecture of Internet scale data and identity systems and markets. This model is intended to tap into the power of stakeholders that are interested in participating in the generation of rules by which their online activity will be governed, rather than merely reacting to rules imposed by governments and others.

The types of stakeholder participation varies because stakeholder interests vary from passive individual and business consumption of data/identity products and services offered in the larger market, to active commercial development of integrated and standardized data/identity solutions. The Participation Governance Model offers everything from educational tools to enhance understanding to inform more passive market participation by consumers of services, to active development tools for use by Trust Framework developers and Steering Groups, to market based information tools to inform policy level discussion and monitoring and auditing activity; and everything in between.

How does the Participation Governance Model relate to Steering Group governance?

The Participation Governance Model helps to define Steering Group *internal* governance by placing it in the context of *external* data/identity stakeholder needs. Toward its goal of providing access and support to all stakeholders, the model provides stakeholders with multiple, independent opportunities to participate in Trust Framework development activities through which legal rules standardization takes place. The Steering Group is one of several vectors through which stakeholders and their representatives can be involved in policy and rule setting (Trust Framework) processes that relate to them. Placing the Steering Group in this development environment can help to clarify its role, which in turn can help to inform its internal governance structure and approach to its future work.

The coordination and collaboration structure of the Participation Governance Model also permits the Steering Group to position itself to have maximum impact on the various issues raised in the NOI. Among these is the ability to generate "authority" for its voluntary standards through the service of providing advice to concurrent Trust Frameworks being developed in the ecosystem/market to help guide their development. In open, voluntary markets for data rights management services and identity/communication services (aka "data/identity" markets), the products and services that best serve all stakeholder needs will be the most broadly adopted products and services. If the Steering Group is to be effective in influencing the direction of such markets, it must establish information feedback loops that enable it to best identify, understand and support multiple stakeholder needs. The Participation Governance Model provides access to such relevant information.

In addition to OIX development of market information tools, Steering Group advisory activities themselves will also provide the Steering Group with important market information that can help to inform its work to identify Trust Framework policy and legal market "best practices" as candidates for standards promotion. Similar to a scaled-up version of a technical standards development mid-level "technical" or "interoperability" committee that reviews the work of multiple working groups for both horizontal and vertical compatibility, the Steering Group can provide a service that helps Trust Framework initiatives to achieve greater interoperability within the ecosystem. This, in turn, can provide the Steering Group with a form of "authority through service" to the extent that it is able to successfully identify and address stakeholder needs. This Steering Group "advisory service" is illustrated in diagrams 7 and 8.

How does the Participation Governance Model compare to traditional technical standard setting?

The Participation Governance Model can be viewed as a "virtualized" standard setting process that is enabled by applying online information sharing and social network tools and the power of stakeholder-guided market mechanisms to the task of bringing together stakeholders to engage in adapted forms of standard setting activity.

Governance and standard setting processes are different for "policy/legal standard setting" than they are for traditional technical standard setting since the desired end product, i.e., the integrated legal duties and rights in Trust Frameworks, is not a set of technical specifications or patent cross licensing arrangements as in traditional technical standards development organizations contexts.

Also, the Internet scale systems legal/policy standards involved require a more comprehensive, inclusive and market-based approach to standard setting, rather than relying on a series of in-person meetings and traditional deliberation and collaboration approaches of a more finite technical initiative that is typically focused on a particular technology or product sector.

How is Trust Framework development work related to the Identity Ecosystem?

Trust Framework development is a form of *standardized rules development* in the networked information system space. It is common practice in many circumstances where the activities and behavior of multiple parties across multiple sectors and with multiple interests are involved to use *legal* frameworks to create integrated multi-contractual structures to address multiple, dependent contracting party rights and duties relating to a specific legal context. "Trust Frameworks" are a type of legal framework that establishes and documents the various uniform stakeholder duties necessary to create "Trust" at scale in networked information systems.

In this context the term "Trust" is held out as a goal that can be fostered through the operation of reliable, predictable data/identity systems that can be "trusted" to help individuals and legal entities to interact with confidence online, whether in a role as data subjects, relying parties, or some sort of third party data handler (including identity providers).[1] In networked systems with multiple stakeholders, "trust" starts with reliability and predictability.[2]

[1] As noted below in Exhibit 2A the "roles" of parties with respect to data vary and are defined differently in different jurisdictions and contexts. For example, in Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (OJ L 281, November 23, 1995)(the "EU 95 Directive") provides definitions relevant to the discernment of the relationship of different parties to data that is not about them. For example, Article 2(d) and (e) of the EU 95 directive defined Data "controller" and Data "Processor" respectively as follows: "Controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations the controller or the specific criteria for his nomination may be designated by national or Community law. By contrast, "Processor" shall mean a natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the controller." The distinction controls with respect to such issues as which party is ultimately responsible for compliance with data protection laws, which company interacts with data subjects regarding issues, which laws apply, and other critical issues. In order to enhance interoperability, when different Trust Framework initiatives are working with definitions of different roles and actions to which their Trust Framework will relate, it is suggested that they consider applying functional definitions from established jurisdictions. This does not require that all Trust Frameworks adopt the default rules of the jurisdictions from which the definitions are borrowed, but just that a form of "normative cross reference" to other sets of definitions, where consistent with the borrower's Trust Framework, can help to establish ties to other data handling systems, which can substantially advance the cause of legal rules interoperability.

[2] The term "trust" has several meanings, which has led some commenters to question its use in policy discussions associated with nascent data/identity markets. Its multiple meanings may, however, be its strength. In the context of online data/identity systems, "trust" can initially be viewed in a mechanistic way, such as in the statement that "I 'trust' my car will stop when I step on the brake." When that "reliable and predictable" mechanistic form of trust is earned, it may foster other forms of "trust" as well. In the case of online, networked information systems, the accomplishment of "trustworthy" systems for handling data, data rights, identity management services, and the like are the initial object of the various "Trust Framework" initiatives. It is through such trusted systems that stakeholders can interact with confidence online in their various roles in social, commercial and political sectors. These forms of "Trust" are prerequisites to full utilization and value creation of networked information systems and online functionality.

A core message of this proposal is that the Steering Group, in its role as a proposed high-level standards-setting entity in the ecosystem,[3] can leverage existing initiatives and resources of the broader community to best achieve its goals. The Participation Governance Model serves to enhance that leverage.

What will Internet scale legal standards look like?

Some data/identity policy/rules standards will have the potential to be applicable at Internet scale across jurisdictions and sectors. Examples might include updated and modified versions of Fair Information Practice Principles (FIPPs)(the standardization of which might support the establishment of a market wide "Level of Control" metric) or standardized rules associated with authentication (that might support the establishment of a market wide "Level of Assurance" metric). At Internet scale, the stakeholder population will be most diverse and the standardized rules will inevitably reflect compromises made to achieve consensus. Those Internet-level principles will initially be quite general to accommodate current variation across jurisdictions, cultures and sectors. As standardization proceeds (driven primarily to cost and interoperability and other "network effect" benefits), the legal principles that are standardized may become increasingly specific and detailed. In either event, robust adoption of the Identity Ecosystem benefits is more likely if stakeholder needs are met (or to the extent that they are not met, where stakeholders perceive that the process can be trusted to have balanced the benefits and to assure the appropriateness of the compromises made).

Processes to discern (and help cohere) stakeholder "needs" at Internet scale at the Trust Framework design and development stage will enhance adoption at the time of Trust Framework deployment. The Participation Governance Model is roughly equivalent to doing "market research" prior to designing a new product or service, but in this case the stakeholders have the capacity to participate in all phases of the product design and development process to the extent that a Trust Framework initiative of interest invites such participation. The Participation Governance Model provides stakeholders with multiple

[3] It is helpful to conceive of the rules standardization "stack" as being like that of the legal "stack" that is present in each sovereign jurisdiction. In the U.S., for example, the top of that stack is the Constitution, with all statutes required to be consistent (upwardly compatible) with the Constitution, further down the stack are regulations that must be consistent with statutes, and still lower in the stack there are enforcement policies that must be consistent with regulations. That public law stack, in turn, is the background against which contracts are entered into by private parties. The contracts can be seen as further down the legal stack, in that they must be consistent with relevant public law. By comparison, in the case of the evolving "data/identity" rules stack, the Identity Ecosystem Framework is roughly equivalent to the "Constitution level," with the anticipation that various Trust Frameworks, at various levels equivalent to statutes, regulations, contracts, etc., are each privately produced "legal standards specifications" that voluntarily choose to be upwardly compatible with the Identity Ecosystem Framework and, as a result, considered part of the Identity Ecosystem "stack." The "upward compatibility" can potentially be achieved through various methods including explicit contractual cross reference or incorporation by reference to specific principles or other requirements of the Identity Ecosystem documentation. This would be the equivalent of a "normative cross reference" in a technical standards setting context.

"Upward compatibility" in the data/identity "stack" may also be achieved through implicit satisfaction of Identity Ecosystem principles, which might be self assessed or subject to confirmation through a third party certification process. It is also likely that compliance with the Identity Ecosystem framework will be relevant information for stakeholders, whether they are data subjects, relying parties or others, and to that extent there could be a formal trust mark process signaling to stakeholders that the tested system conforms to Identity Ecosystem standards. Those same certification and marking considerations apply to all other Trust Frameworks in the "data/identity stack."

pathways to participate. The design and development process must be scalable to accommodate multiple stakeholders' diverse interests.

As noted elsewhere in this NOI response, because Internet scale solutions necessarily involve multiple jurisdictions, enforceable legal duties will be set forth in voluntary standardized contracts, rather than in laws and regulations. Laws only apply within jurisdictions. Contracts can bridge jurisdictions.

Viewed in its entirety, the Participation Governance Model process is a form of "crowd sourced" self-regulatory rule setting through which stakeholders can collaborate at either more "local" or Internet scale. Stakeholders from all perspectives can leverage existing commercial, international and community-based standards with broad information sharing, online collaboration and education, and market-based tools and programs. In doing so all stakeholders have the opportunity to help create enforceable rules to which they are then bound, consistent with the NSTIC vision of private sector leadership, that will ensure them reliable, predictable, secure, privacy preserving, and interoperable data/identity infrastructure.

The Participation Governance Model saves costs and leverages private sector resources

The position of the Steering Group in the larger participation structure is also most conservative with resources, and will save costs for all participants. This is because it permits the Steering Group to take maximum advantage of existing resources and to simultaneously leverage and support the work of other existing private initiatives (such as technical and related standards development organizations, providers of deployed Trust Frameworks, academic research and pilot projects, etc.) across the Internet and related networked information systems.

The Participation Governance Model encourages stakeholder participation at a number of levels, and provides collaboration tools for future stakeholder participation, effectively "crowd sourcing" tough issues and, through that rulemaking process, raising stakeholder awareness and bridging currently separate jurisdictions and social, commercial and political sectors.

This material describes the Participation Governance Model and the way in which it can support NSTIC goals, including helping to meet those governance challenges outlined in the NOI.

Are the structures of the Participation Governance Model already being built?

The first part of the Participation Governance Model has already been carried into practice in the form of OIX programs and tools that are currently available to all Identity Ecosystem stakeholders and the public at www.openidetityexchange.org . The OIX Trust Framework development tools support Trust Framework initiatives in each of the 5 steps of "rulemaking" activity that are part of building a Trust Framework. The Trust Framework Metadata Listing Service supports deployment of Trust Frameworks, and the establishment of a "market" that provides an important form of stakeholder group "feedback" to inform future Tools and Rules modifications supporting a "race to the top" where rules best practices can be standardized across currently siloed systems. The rule setting tools are all ready fully available on the OIX website, and the programs are already underway. The model, and the OIX programs and tools that support it, are fully consistent with the NSTIC vision.

The establishment of a private-sector-led Steering Group will provide the important country/jurisdiction policy feedback mechanism to inform Trust Framework development in open data/identity markets, and will complete the assembly of the basic components of the Participation Governance Model, enabling the processes to achieve the Identity Ecosystem end-state envisioned by NSTIC.

What existing work can be leveraged to help initiate the Steering Group?

As part of the OIX goal to enhance interoperability across data/identity systems carried on networked information systems, OIX offers all stakeholders and the public free access to all of its online tools. The intention is that when different stakeholders use the same tools for analyzing, designing and developing separate Trust Frameworks, interoperability will be enhanced. Commonality in design, analysis, definitions, metrics, terms and even governance structures can help systems to achieve "legal interoperability" across previously stove-piped jurisdictions and industry sectors.

As an example of how existing work can be leveraged, in Diagram 4 the suggestion is made that the Steering Group governance discussions leverage the "Smart Grid Interoperability Panel Governing Board and Smart Grid Interoperability Panel Charter" (the "Smart Grid Charter") as a starting point for deliberation about the NSTIC Steering Group governance structure.

The Smart Grid Charter document will clearly require substantial modifications to account for such differences as the ready availability to the Steering Group of OIX programs, tools, and other OIX "information plumbing," (the likes of which wasn't already available to the Smart Grid stakeholders for their work in electricity markets), and to account for the different contexts in which the two networks are being developed (U.S. domestic regulated electricity system versus data/identity networks carried on the Internet). However, since networked systems in different sectors display many similar characteristics,[4] it appears that the hard work done by the individuals and institutions involved in putting together the Smart Grid's SGIP charter document can help "jump start" the effort in the Steering Group context. This warrants using the SGIP charter as a NSTIC Steering Group "first draft."[5]

How does OIX support the Participation Governance Model and the NSTIC goals?

The Open Identity Exchange was formed and is operated to provide a platform for open, public information exchange, the identification of "best practices," and candidates for rules standardization associated with data and identity markets at Internet scale. It is a not-for-profit corporation committed in its official corporate purposes to making data/identity market-relevant information broadly available to stakeholders and the public and improving conditions in the data/identity markets generally. OIX is technology neutral, jurisdiction independent, open, transparent and stakeholder inclusive.

[4] See, for example, "Networks, Crowds and Markets" by David Easley and Jon Kleinberg (Cambridge Press, 2010) for a discussion of Graph Theory, Game Theory, Markets, Theories of Strategic Interaction in Networks, and Network Dynamics Models which apply across networks in different domains.

[5] See APPENDIX C for a redlined version of the Smart Grid Charter showing suggested changes to form a initial discussion draft of a potential NSTIC Steering Group charter. The draft has already been posted on the OIX website at http://openidentityexchange.org/white-papers and has elicited comments that are available for review by NOI responders and the public. The draft is a governance "checklist" in charter form.

Existing OIX programs and tools are directed at supporting the development of "Trust Frameworks." Trust Frameworks are integrated sets of rules, set out in standardized multiparty contracts, that provide uniform standards of behavior (through enforceable legal duties) for stakeholders relating to the actions that they take when handling data that potentially affect the data rights and identity/communications integrity of other entities in networked information systems.[6] Uniform agreements support uniform duties across information networks and the data/identity systems that are carried on those networks.

[6] OIX has made tools publicly available to assist individuals and entities in understanding and "self-audit" of data actions that they take or which are taken on their behalf. The data action survey tool is an example, and is available at http://openidentityexchange.org/join.

# ***Part I: The Participation Governance Model***

## OVERVIEW OF THE DIAGRAMS

The Participation Governance Model is intended to promote a healthy, sustainable, transparent Identity Ecosystem. Included below are eight diagrams that together provide a general overview of the Participation Governance Model with emphasis on the place of the NSTIC Identity Ecosystem and the Steering Group in the model and represented in the diagrams.

The diagrams start out with the basic NSTIC Identity Ecosystem diagram and then describe different supporting structures and processes that can help the vision of the NSTIC to be realized.

The Purpose of this Part 1 is to provide an overview and virtual "tour" of the model through use of the diagrams. Toward that end, the narrative that follows each of the eight diagrams is divided into the following categories:

Purpose of Diagram
Brief Explanation
Tour of the Diagram
Additional notes relating to Diagram

# TABLE OF DIAGRAM TITLES

The following Table of Diagram Titles is intended to provide an orientation to the entire set of diagrams through their descriptive titles.

Diagram 1 – **Identity Ecosystem as Conceived by NSTIC** (Diagram from NSTIC p. 26)
Showing a snapshot of the "end-state" of the U.S. Identity Ecosystem post-NSTIC implementation

Diagram 2 – **Rulemaking Steps to Building NSTIC Identity Ecosystem**
Showing the 5 stages of rulemaking that are part of all Trust Framework development

Diagram 3 – **Developing the Trust Framework Components of an Identity Ecosystem**
Illustrating Trust Framework development pathways, and the support of OIX programs and tools

Diagram 4- **Smart Grid: A Potential Model for Steering Group Governance**
Depicting the Smart Grid Interoperability Panel and Governing Board model; a possible starting point for Steering Group governance

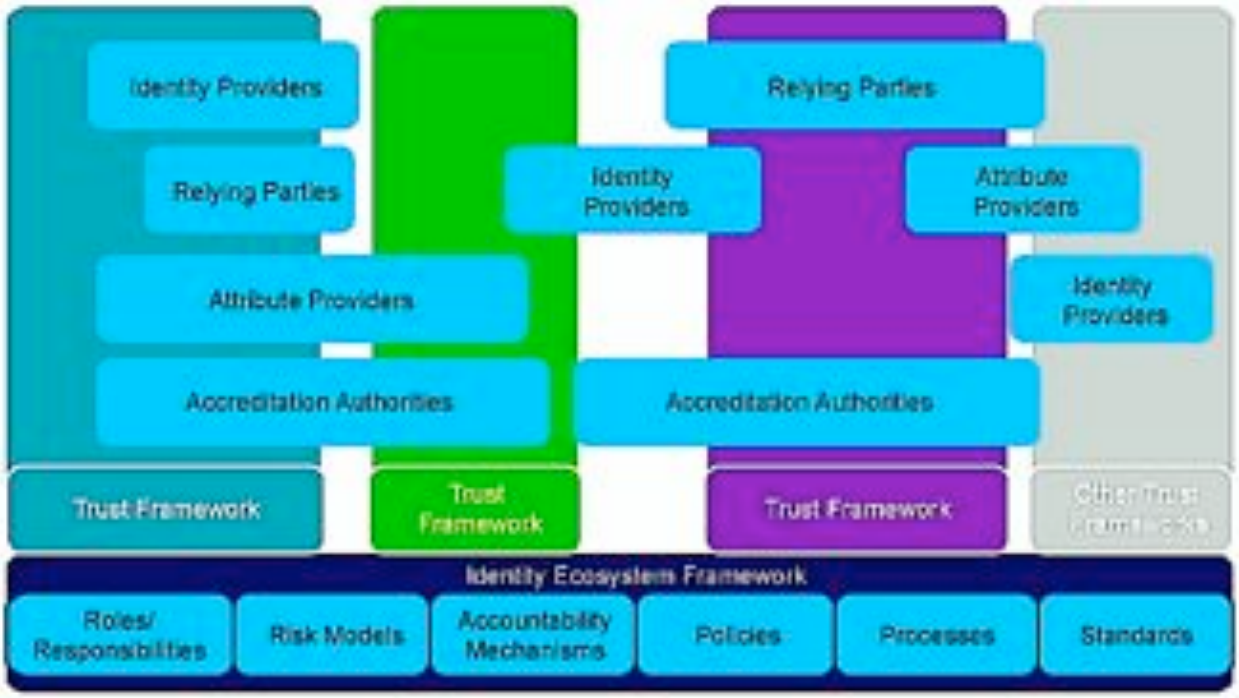
Diagram 5 - **Pathways to Stakeholder Participation**
Visualizes the multiple vehicles through which data/identity system participants in various stakeholder roles can participate in rule setting and policy development for data/identity products

Diagram 6 - **Steering Group Initiation**
Isolates attention to how the development of Steering Group governance structure can be conceived of as a form of 5-step rulemaking

Diagram 7 - **U.S. Steering Group Participation in the Identity Ecosystem**
Illustrates how the Steering Group can use OIX programs and tools to interact with various Trust Framework initiatives to provide guidance and direction to the market

Diagram 8 - **International Initiatives Participation in the Identity Ecosystem**
Duplicates the interaction shown in Diagram 7 to multiple Trust Frameworks, each offering Trust Framework initiatives guidance, advice and possibly certification to encourage adoption of the duties and rules of their respective Identity Ecosystems

**Diagram 1 - Identity Ecosystem as Conceived by NSTIC**




Purpose of Diagram:
To illustrate the U.S. NSTIC once adopted and implemented.

Brief Explanation:
A sustainable, secure, efficient, interoperable "Identity Ecosystem" is the desired end-state of the NSTIC. The NOI calls for governance models for the private sector Steering Group that will support NSTIC. The Participation Governance Model that is supported by OIX tools and programs can help to define Steering Group function that in turn can inform Steering Group internal governance and process structures. It is therefore appropriate to start with the diagram of the "Identity Ecosystem" end state set forth in the NSTIC and use that diagram as a jumping off point for the description of the Steering Group governance proposal.

Tour of the Diagram:
This diagram is substantially similar to that set forth in the original NSTIC proposal (at page 26 of the print copy) as signed by President Obama on April 15, 2011. The NSTIC document does not offer a detailed description of the diagram, but it appears to be intended to show a snapshot of a hypothetical, representative set of stakeholders and overall structure. In this way, it also represents the NSTIC-desired, fully implemented, interoperable end-state of the work of the Steering Group along with all other stakeholders in the Identity Ecosystem.

There are several notable elements of the diagram, including:

It anticipates multiple separate but interoperable Trust Frameworks in the ecosystem (each indicated by the vertical bars in the diagram).

It anticipates that stakeholders (indicated by horizontal bars), such as, but not limited to, RPs, IDPs, APs, and Accreditation Authorities, as illustrated in the diagram, may rely on one or several Trust Frameworks when they act in their respective roles online.

It anticipates that there are online activities that take place outside of Trust Frameworks, but still within the Identity Ecosystem that is within U.S. NSTIC auspices[7] (as indicated by the white space enclosed by the dotted line.

It allows for (although it is not explicit on this point), other similar "Identity Ecosystems" (that might exist outside of the diagram's dotted line) that are independent of that of the U.S. NSTIC-consistent Identity Ecosystem. It is anticipated that, at least in the early periods of development, different countries may opt to develop parallel systems to that of the U.S. This is undesirable for the overall data/identity sector, since it merely continues current jurisdictional silos (such as that between the EU and U.S. associated with the rules for handling "personal information").

Notwithstanding its undesirability from an interoperability and efficiency point of view, multiple jurisdictional silos in the early period reflects the reality that the benefits of Trust Framework and Identity Ecosystem Framework "network effects" and benefits of scale from legal interoperability have not yet been matured to the point that they are broadly recognized to offer a compelling economic reason to align legal rules across jurisdictions. It is anticipated that the emergence of a set of core standard legal rules will take some time.

OIX programs and tools help stakeholders to review data/identity market related information to help each of them to identify "best practices" that can provide candidates for standardization. That standardization may take place in many ways, for example through the form of formal promotion of a standard, through the normative reference to a standard in a Trust Framework, or the adoption by multiple parties of a proprietary offering of a single company, or the conformity of one or more stakeholders to the rules imposed by the laws of a jurisdiction. Each is a form of standard, and each will take some time to develop. The Steering Group offers a structure through which high-level standards can be promoted that can help to guide broad markets.

[7] The word "auspices" here is used to convey the distinction between U.S. sovereign national legal jurisdiction and the relatively looser and broader reach that is anticipated to arise under the relatively unusual scenario where NSTIC is a government strategy intended to engender private, Internet scale rules and duties standardization; with the U.S. Steering Group offering a non-compulsory standard intended to attract the adoption of multiple Trust Frameworks (that will each normatively cross reference U.S. NSTIC standards in their respective Trust Framework documents) and thereby promote policy/legal interoperability for those system characteristics that are associated with those broadly adopted policies. In this scenario NSTIC-derived standard duties and rights may affect both U.S. citizens, U.S. residents, and legal entities with U.S. nexus, as would be expected, as well as the rights and duties of stakeholders that voluntarily accept NSTIC-consistent rules when they develop or join Trust Frameworks that are formed outside of U.S. legal jurisdiction. It is generally akin to the situation where a foreign person buys stock of a public company that files its securities reports consistent with U.S. generally accepted accounting principles (GAAP). That person is not subject to the legal jurisdiction of the U.S., but enjoys the advantages of the reliability offered by GAAP compliance through their purchase of the stock. A member of a Trust Framework, wherever it was formed, that complies with NSTIC standards will enjoy similar benefits of reliability and predictability.

The Diagram also offers a listing of other elements of the Identity Ecosystem that are not either stakeholders or Trust Frameworks. These are listed on the dark blue bar at the bottom of the diagram and are indicated to be part of the "Identity System Framework." These include: "Roles/Responsibilities, Risk Models, Accountability Mechanisms, Policies, Processes and Standards." The exact nature of each of these elements is not described in detail, but is appropriately left for the Steering Group to work on with relevant stakeholders. The NSTIC does provide that:

> Figure 4 illustrates multiple Trust Frameworks built upon the foundation of the Identity Ecosystem Framework. This baseline ensures underlying interoperability such that credentials can be relied upon even when the participants are in different Trust Frameworks.

The description of Figure 4 establishes the notion that the Identity Ecosystem is built on the scaffolding of an Identity Ecosystem Framework. It is not coincidental that the Framework metaphor is invoked here, given that the Identity Ecosystem is itself populated by multiple Trust Frameworks, each of which is required to be compatible with the standards of the Identity Ecosystem Framework if it is to be considered part of the Identity Ecosystem. Participation is not compulsory, but compliance with its standards is compulsory once a party voluntarily decides to join. It is like the situation where a consumer is not required to apply for a particular credit card, but if he/she does so, he/she will be bound to its standardized terms.

Additional notes relating to Diagram:
The NOI provides that:

> The Identity Ecosystem is an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities and the digital identities of devices. The Identity Ecosystem Framework is the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that govern the Identity Ecosystem.

The NSTIC graphic at page 26 is that of a hypothetical Identity Ecosystem. It represents the "Identity Ecosystem" end state; mature, but subject to further updating as circumstances change.

The "Identity Ecosystem" definition establishes important criteria for Steering Group work and governance in its acknowledgement that the Identity Ecosystem is an "environment" in which individuals and organizations interact. The outer bounds of that "environment "" are identified by the dotted lines in the diagram. The "environment" is external to any of the individual stakeholders that occupy it. That external data/identity ecosystem "environment" already exists, and stakeholders are already interacting in it, but it does not yet manifest all of the qualities that are called for in NSTIC, nor all of the qualities desired by its many stakeholders.

Once it is formed, the Steering Group will join the individuals and organizations that are already interacting in the Identity Ecosystem, and will pursue the goals set forth in NSTIC in an effort to improve the ecosystem to better serve the needs of its stakeholders. It will be another participant, albeit one with a broader, system-oriented role of identifying best practices and promoting their formalization into standards that can support the vision, guiding principles, goals and objectives and actions contemplated in NSTIC. That role is consistent with private interests already interacting in the ecosystem who seek to achieve reliability, predictability, interoperability and other goals of normalized market functioning.

Most system stakeholders (such as individuals, businesses and governments acting as relying parties (RPs), data subjects and data handlers) in the system were not created specifically for the purpose of interacting in the identity ecosystem, but find themselves in that position because of the benefits of using networked information systems for a variety of online and offline pursuits. By contrast, the Steering Group as an entity is being designed to perform a specific set of functions with respect to the ecosystem. It is acting to help realize the vision of NSTIC to the benefit of stakeholders that participate in the Identity Ecosystem. Its goals are defined entirely by the needs of other stakeholders. That special role driven by external factors can help to inform the design of its internal organization and operation.

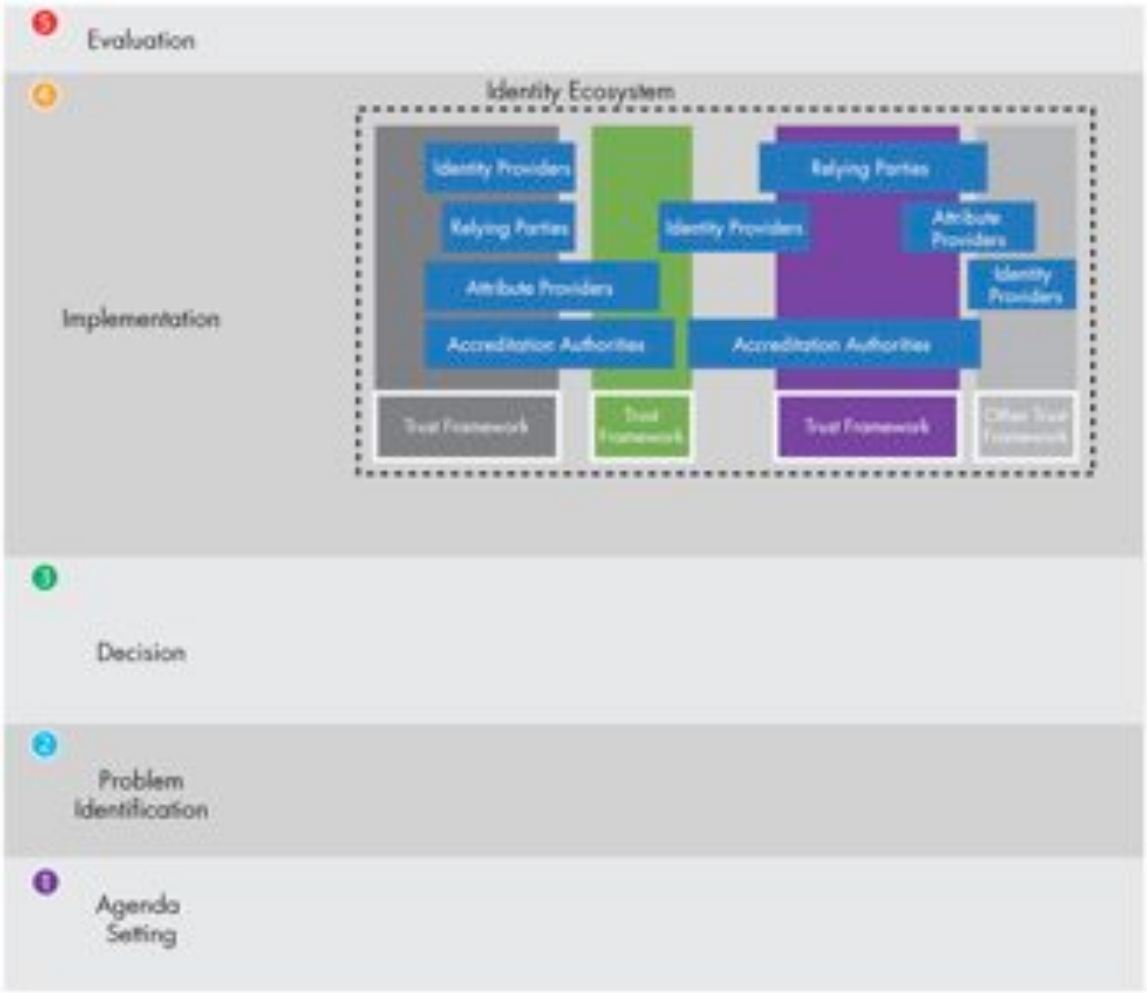
The acknowledgement of the external goals and roles of the Steering Group helps to provide additional clarification on how the internal mechanisms of the Steering Group might be most effectively configured. In other words, the internal processes of the Steering Group should be defined by the external ecosystem and its needs. The balances of the diagrams (Diagrams 2-8) provide increasingly broader views applying the Participation Governance Model of the support systems for the Identity Ecosystem and the role of the Steering Group within that ecosystem.

For example, the Steering Group will not seek to create a new ecosystem. Instead, it will help integrate the existing systems to enhance functioning that serves the needs of its stakeholders consistent with the NSTIC. Given its role as a private body and the reality of the global scope of Internet-based networked information systems, the Steering Group is limited to persuasion, rather than compulsion, as the mechanism to coax conformity to standardized rules. This "opt-in," voluntary model of standard setting immediately suggests that standardization will depend upon broad rules adoption. Adoption itself will be fostered if stakeholder needs are well understood at the inception of the rule setting exercise, so that they can be addressed in deployed rules systems. This counsels in favor of an open, participation model such as the Participation Governance Model.

To support an open model, the internal processes of the Steering Group should be structured to permit and encourage broad stakeholder participation (which is akin to a structured form of "crowd sourcing," if you will), of what will become a perennial rules construction exercise as it continues to be necessary to define new duties to support new rights of stakeholders as the pace of change brought about by increasingly networked information systems continues to accelerate. This proposal suggests that, in order to save time, money and resources during initiation, the Steering Group should be structured so that it can best avail itself of existing systems that have been put in place to enable that broad participation, such as the programs and tools of OIX, and the work of existing standard setting initiatives in the data/identity space and adjacent fields that have each started to develop specific legal standards within their respective Trust Frameworks that could be candidates for Identity Ecosystem-level standardization. The diagrams illustrate the layers of support that are applied in the Participation Governance Model.

The Steering Group will not directly *steer* the entire ecosystem (although it may influence it by promoting standards that are viewed as broadly beneficial across jurisdictions). Instead, it will steer U.S. based policy (and the policies of those countries, industries, institutions and individuals that voluntarily "opt-in" to the NSTIC Steering Group standards to enjoy its benefits), within the larger ecosystem.

**Diagram 2 –Steps to Building NSTIC Identity Ecosystem**




Purpose of Diagram:
Diagram 2 places the NSTIC "Identity Ecosystem" end state in the context of the overall rule setting processes that will be required to create the Trust Frameworks that make up the ecosystem.

Brief Explanation:
The NSTIC "Identity Ecosystem" diagram is shown on a generic rule setting process timeline as the "implementation" that follows the processes of "agenda setting," "problem identification," and "decision," and which precedes "evaluation" which then can feed back into agenda setting for new issues to be addressed.

Tour of the Diagram:
The Identity Ecosystem policy development process is presented overlaid on a chart that illustrates the five stages of rulemaking in the public/private context, borrowed from policy sciences literature.[8] Each

[8] These five stages are borrowed from policy sciences literature. In particular, the overall conceptual framework derived in the article "Self-regulation as policy process: The multiple and criss-crossing stages of private rule making" by Tony Porter &

of these stages, and the rule setting process overall, will lead to potential opportunities and challenges for the commercial and governmental sector (and the NSTIC and OIX initiatives in particular), in each stage and in the overall rulemaking process. Drawing stakeholder attention to the stages of the process and the various potential opportunities and challenges can help all participants to better coordinate their efforts in the area.

The five stages of rulemaking are:

*Agenda Setting* (discussion of issues),
*Problem Identification* (focusing on relevant variables in the discussion),
*Decision* (definition of future action items),
*Implementation* (focusing on deployment), and
*Evaluation* (assessment of implementation and new *agenda setting* cycle)

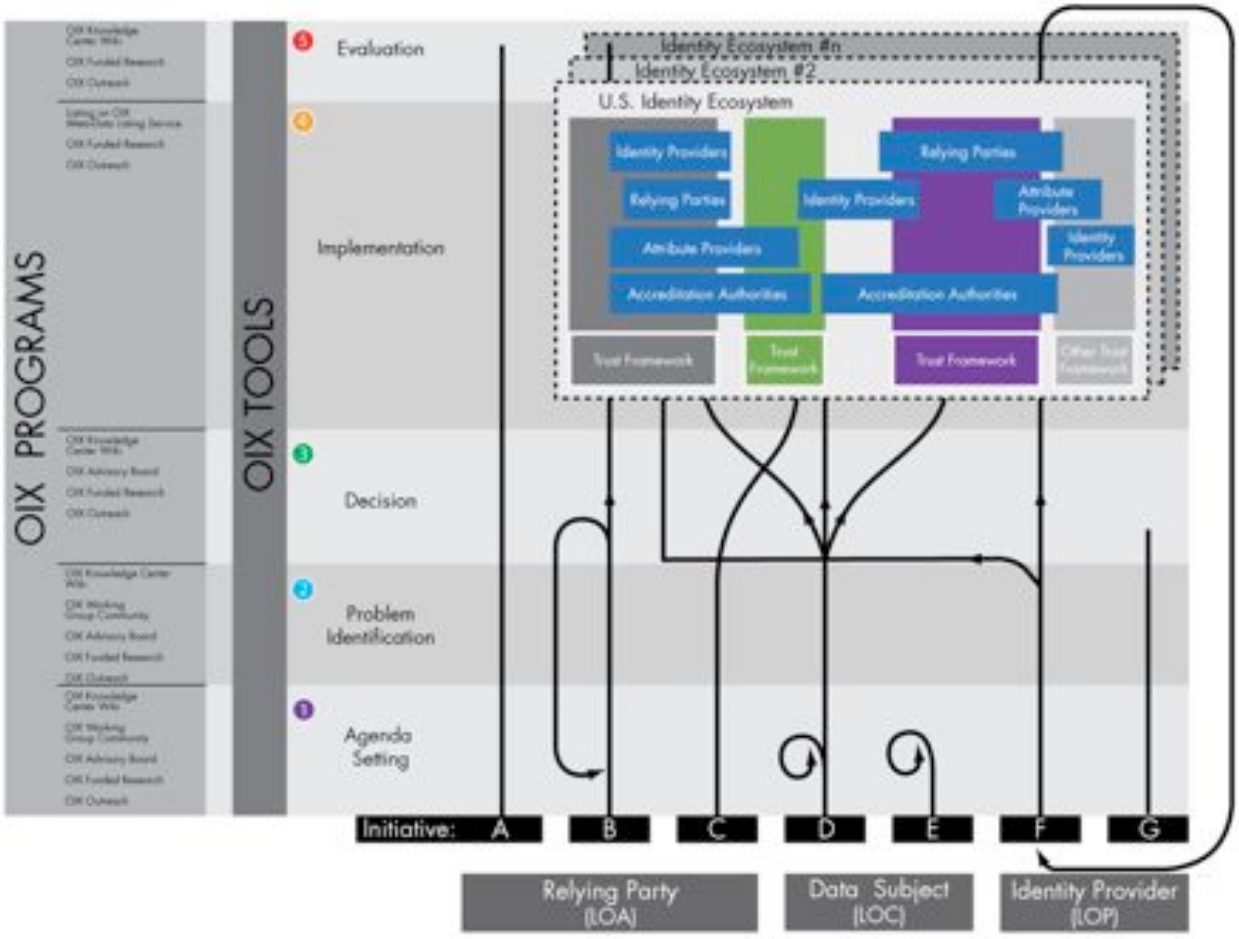
Commercial and governmental roles vary in type and intensity at each stage of the rule setting process, and from one rules setting context to another. Hopefully though correlating both NSTIC and OIX programs with this empirically-derived, 5 stage, rule-making construct, the natural alignment of the respective programs will become clearer, enabling greater coordination to the benefit of both programs.

A more detailed overview of each of the rulemaking steps is provided in Exhibit 2A.

Additional notes relating to Diagram:
Please see Exhibit 2A

Karsten Ronit (Policy Sciences, 2006) (Ronit 2006), is relied upon for the basic structure reflected here. That article surveyed dozens of hybrid public/private rule making settings in various countries to derive the five stages that are applied here.

**Diagram 3 - Programs and Pathways to Trust Framework Development**




Purpose of Diagram:
Diagram 3 illustrates how individual (hypothetical) Trust Frameworks initiatives (a.k.a. "networked information system rule setting initiatives") in the Identity Ecosystem follow development pathways leading to the deployed Trust Frameworks that together populate the Identity Ecosystem end state. It also shows how OIX programs and tools support each stage of rules development for each Trust Framework development initiative.

Brief Explanation:
Diagram 3 maps hypothetical Trust Framework development pathways onto the 5 five stage rulemaking process, and illustrates how those different Trust Framework initiatives, rooted in different user group needs, interact to inform the "Trust Frameworks" that are represented by the vertical bars in the NSTIC Identity Ecosystem diagram (Diagram number 1).

Diagram 3 also introduces (on the left side) the various OIX programs and OIX Tools that support Trust Framework and Ecosystem Framework development activity at each stage of the rule setting process.

The promotion by OIX of common tools and programs enables broad collaboration, and the use of such tools can promote greater interoperability by bringing separate Trust Framework initiatives together,

and by offering a common analytical framework for use across initiatives. The "data-action-based" analytical structure employed by the tools can be applied to systems across legal jurisdictions and industry sectors.

Tour of the Diagram:

Since this diagram introduces several new elements, the "tour" will start in the upper right hand side of the diagram and then separately describe the lower right hand side and finally the left hand side of the diagram.

The NSTIC "Identity Ecosystem" diagram (Diagram 1), and the five rulemaking stages from Diagram 2 are brought forward as the foundation for Diagram 3.

Upper right quadrant of Diagram 3:
A new addition in Diagram 3 is the presence of additional, alternative Identity Ecosystems that are expected to develop as a result of the presence of other sovereign jurisdictions imposing their respective local laws, which may have the effect of creating barriers to interoperability with the U.S. Identity Ecosystem. Although there is broad interest in bridging these jurisdictional gaps, it is recognized that, at least in the initial phases of Internet-scale data/identity systems, differences will be present as a result of different legacy legal structures (and stakeholder expectations in such jurisdictions) associated with current different sovereign jurisdictional silos. Accordingly, it is possible that these Identity Ecosystems may be comprised of actors in particular countries (such as the U.S.), groups of countries (such as the EU or APEC) or, at a lower level, substructures of sovereign nations (such as provinces, states, etc.).

These separate alternative Identity Ecosystems can be made interoperable by enabling each to seek common "tools and rules." The Participation Governance Model provides a structure for such inter-sovereign collaboration through a multiparty Steering Group Structure that is illustrated in Diagram 5.. A Steering Group that includes representation of stakeholders from multiple Identity Ecosystems can facilitate the identification and creation of common tools and rules to make different Identity Ecosystems interoperable. It is hopeful that such efforts can lead to the creation of Trust Frameworks that transcend particular Identity Ecosystems. These Identity Ecosystems may include countries (such as the U.S. Identity Ecosystem), groups of countries (such as the EU or APEC) or, at a lower level, substructures of sovereign nations (such as provinces, states, etc.).

Lower right quadrant of Diagram 3:
The lower right quadrant of the diagram illustrates the "growth patterns" of seven separate hypothetical Trust Framework initiatives (A through G) as they proceed through the five rulemaking stages.

Note that each initiative is shown as contiguous with one of three typical roles in data/identity systems.[9] The diagram suggests that each Trust Framework initiative, and the Trust Framework rules that they produce, originates from a particular data "role" perspective.

[9] It is recognized that the roles described as "Relying Party," "Data Subject," and "Identity Provider," indicate an origin in the description of identification, credentialing and authentication context. These are not the exclusive roles that stakeholder might assume in data/identity systems, but they are typically applied since much discussion at present is focused on the establishment of "trust" online, and hence the initial authentication and related processes needed to achieve that trust. In the broader data and identity contexts, there are other roles such as the EU concepts of data "controllers" and "processors," state

From its origin in one of the three roles, each Trust Framework development initiative grows through the 5 rulemaking stages, sometimes remaining in one stage for an extended period before proceeding (see, for example, initiative "E").

For simplicity in the diagram, three gross categories of roles are presented including the relying party ("RP") (the duties owed to RPs are colloquially referred to by the system metric "level of assurance" or LOA); the data subject ("DS") (the duties owed to DSs are referenced as "levels of control" or LOC); and the identity provider ("IDP") (the duties, such as relying party best practices ("RPBP"), owed to IDPs are referenced as "levels of protection" of LOP).

These are not exclusive categories, and some Trust Frameworks are intended to address multiple vectors. The current reality appears to be, however, that there are fewer Trust Frameworks that are intended to comprehensively address all of the roles. Instead, some proposals for Trust Frameworks that were previously imagined to be comprehensive are now being recognized as having insufficiently addressed the needs of multiple stakeholder roles, an exercise that must now be engaged in if they are to get additional traction.

An example is the U.S. Federal Identity, Credential, and Access Management ("FICAM") program that provided a thorough treatment of the U.S. Government's statement of its needs as a relying party, but did not fully establish other system requirements associated with DS and IDP needs.[10] As a result, the program requirements are still being ironed out, particularly at higher levels of assurance.

The categories are not rigid, but are intended to illustrate that, to date, a given Trust Framework development initiative is typically energized by one or another of the roles, but not all. One of the purposes of NSTIC is to establish a Steering Group that can take a more comprehensive view and help to knit together the single-role Trust Frameworks into more integrated, multi-role rule sets, ultimately providing guidance on the operations of the Identity Ecosystem. As noted elsewhere, comprehensive Trust Frameworks offer the benefit of being able to scale by creating enforceable legal obligations among the parties based on the exchange of promises as contractual consideration, rather than having to identify other required contractual consideration to support a binding contract.

The following is a brief narrative explanation of several of these illustrative Trust Framework development pathways:

*Initiative A*:
Initiative A is primarily associated with the RPs needs (measured by the LOA metric). This might arise, for example, where a party is developing a Trust Framework specification solely associated with identity authentication and other relying party needs. Initiative A proceeded through the 5 stages. Such a Trust

---

data breach concepts of "data owner" and "data licensees," other roles that can also be conceived of as being the source of future Trust Framework development initiatives.

[10] Notably the FICAM and Trust Framework Provider Adoption Process ("TFPAP") materials did provide assesors with draft guidelines on privacy issues, which were intended to address some of the types of issues that would go into consideration of an LOC metric for the benefit of individual data subjects. The inclusion of that material could be seen as qualifying the FICAM/TFPAP material as addressing LOA and LOC needs from the government's perspective. It did not, however address various IDP needs, like RP-BP, which would inform an LOP metric.

Framework would be useful in a closed-system B2B setting. Also, where such B2B LOA solutions are available to be evaluated in an open market, they might be normatively cross referenced by other solutions (for instance those developed from the LOC perspective, to together form the elements of a more comprehensive Trust Framework solution that simultaneously addresses RP, DS and IDP needs by creating an integrated structure of duties on RPs, DSs and IDPs. The fact that the development path for Initiative A does not intersect with the Identity Ecosystem boxes in the upper right of the diagram, suggests that it incorporated some element that is not consistent with the U.S. Identity Ecosystem or any of the other Identity Ecosystems. Thus, for example, if all Identity Ecosystems in the future required some portability rights for data subjects, a high security B2B solution might not satisfy that requirement. Since participation is voluntary in the Identity Ecosystem, this is okay, but the parties that apply Initiative A will not experience the "network effect" benefits of interoperability with the Identity Ecosystem. It is expected that the "network effect" will result in the economic incentive for Initiative A to align with one or more Identity Ecosystem Frameworks. This may not matter to the promoters of Initiative A, who might merely have sought to create a purely security and system integrity oriented B2B Trust Framework.

*Initiative B*:
Initiative B also started in the RP context (LOA oriented). Initiative B experienced an "issue split" at the Decision stage. At that stage some of its issues proceeded to implementation and are shown (through intersection) to be consistent with the various Identity Ecosystems (indicated by the arrow from B that continues to climb though the various Identity Ecosystem boxes). However, it appears (from the curved descending arrow) that some issues were identified as unresolved at the decision stage and returned to the "agenda setting" stage, where they will be further refined, analyzed and prepared for later promotion through the rule setting process.

*Initiative C*:
Initiative C also started from an RP orientation. The Trust Framework being developed by initiative C was developed and then is shown to have been implemented in the second Trust Framework of the NSTIC Identity Ecosystem diagram.

*Initiative D*:
Initiative D started from the Data Subject perspective. Examples of Data Subject oriented Trust Frameworks include those based on FIPPs and other structures that are intended to address individual or institutional data subject needs.[11] Initiative D has an issue that remains in the agenda setting stage (as indicated by the curved arrow that branches off of its development pathway during the agenda stage). Other than the issue that remains in "agenda setting" it appears that the Trust Framework created by Initiative D is very popular. It has been adopted by three separate Trust Frameworks in the U.S. Identity Ecosystem (as indicated by the three-prong fork that occurs at the decision stage of the Initiative D pathway).

*Initiative E*:
Initiative E also is starting from the data subject perspective. It remains for now in the agenda setting stage. This might be characteristic of an initiative that is just getting started, or an issue that would

[11] Although LOC is most frequently associated with individual data subject needs, and FIPPs is clearly geared at the needs of individual data subjects, it is readily apparent that entity data subjects (such as companies, governments, etc.) will involve some issues of "identity integrity and control" that will not be identical to those of individual data subjects.

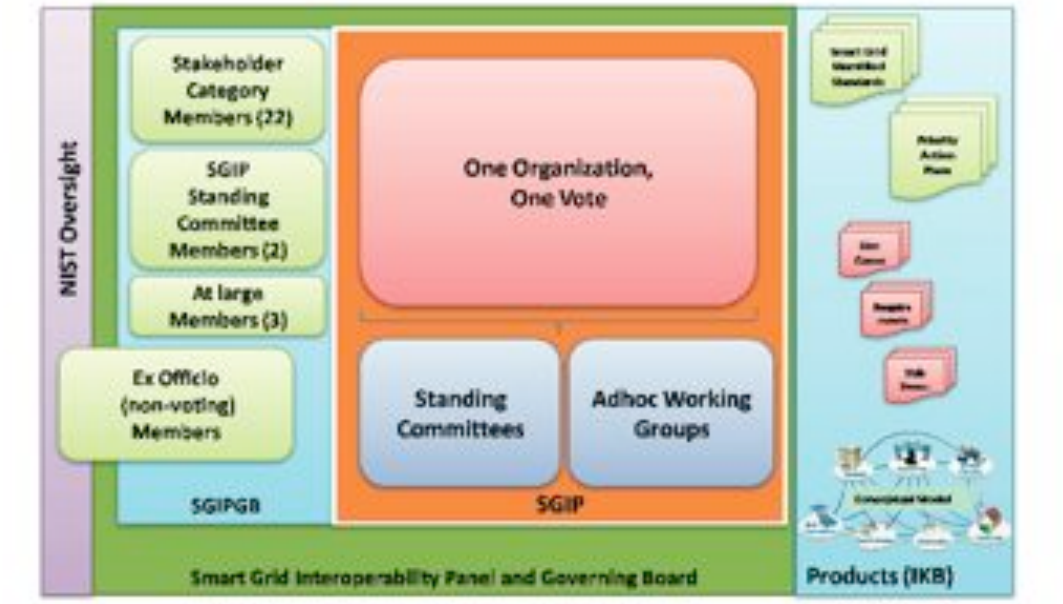
benefit from extended discussion and community interaction before one or more of its issues are promoted to the "problem identification" stage.

*Initiative F*:
Initiative F started from the IDP perspective. This might include such LOP requirements as relying party best practices (RP-BP), and also duties placed on data subjects associated with limiting credential usage and the like. In both cases the standard duties are intended to make data/identity systems more secure and to increase system overall performance integrity. Initiative F has also been successful; being as it has been adopted by two of the Trust Frameworks shown in the U.S. Identity Ecosystem diagram. Notably, Initiative F is sufficiently mature that it has already reached the evaluation stage, which has resulted in some issues being returned to agenda setting for further rules development. This is indicated by the long arrow that runs down the right side of the diagram and returns to the bottom of the "F" box. This might take place, for instance, if technology changes render anachronistic some part of the rules in the Initiative F Trust Framework.

*Initiative G*:
Initiative G has only gotten to the decision stage. It is in the process of preparing and drafting its Trust Framework documents to reflect its work at the agenda setting and problem identification stages.

Left hand side of Diagram 3:
Finally, the diagram introduces the support structure of OIX programs and tools, which provide different types of support and opportunities for participation in each of the different rule setting stages. A complete description of OIX programs and tools can be found at www.openidentityexchange.org

**Diagram 4 – Smart Grid: A Potential Model for Steering Group Governance**




Purpose of Diagram:
To introduce the Smart Grid Interoperability Panel and Governing Board (SGIP and SGIPB) as a consensus-recognized "straw man" proposal for discussions of a model NSTIC Steering Group governance structure.

Brief Explanation:
On July 13, 2011 representatives of a diverse swath of over a dozen Identity Ecosystem stakeholders convened in Washington, DC to debate and ratify any points of consensus on NSTIC Steering Group governance structures. The discussion yielded 10 Points of Consensus (the "July 13 Ten Points of Consensus"), which can be found at Exhibit 4A. Of the July 13 Ten Points of Consensus, one was that the Smart Grid model, is sector specific, yet useful model of phased development of a governing system.

This Diagram 4 will serve as the "stand in" icon in the balance of the Participation Governance Model diagrams for what the U.S. NSTIC Steering Group could look like. OIX has provided, at APPENDIX C, a redlined version of the Smart Grid Charter altered to provide a model of a starting point for NSTIC-consistent, Identity Ecosystem Steering Committee governance.

Tour of the Diagram:
The diagram is presented for discussion purposes only, but the Smart Grid public-private partnership model featured several structural points that may be helpful in considering structures for Steering Group governance (such as an active plenary structure, a supportive governing board, and consensus-seeking processes) as well as a phased development of governing structures, consistent with the July 13 Ten Points of Consensus and with the 5 stages of rulemaking analysis, applied to Steering Group governance rules.

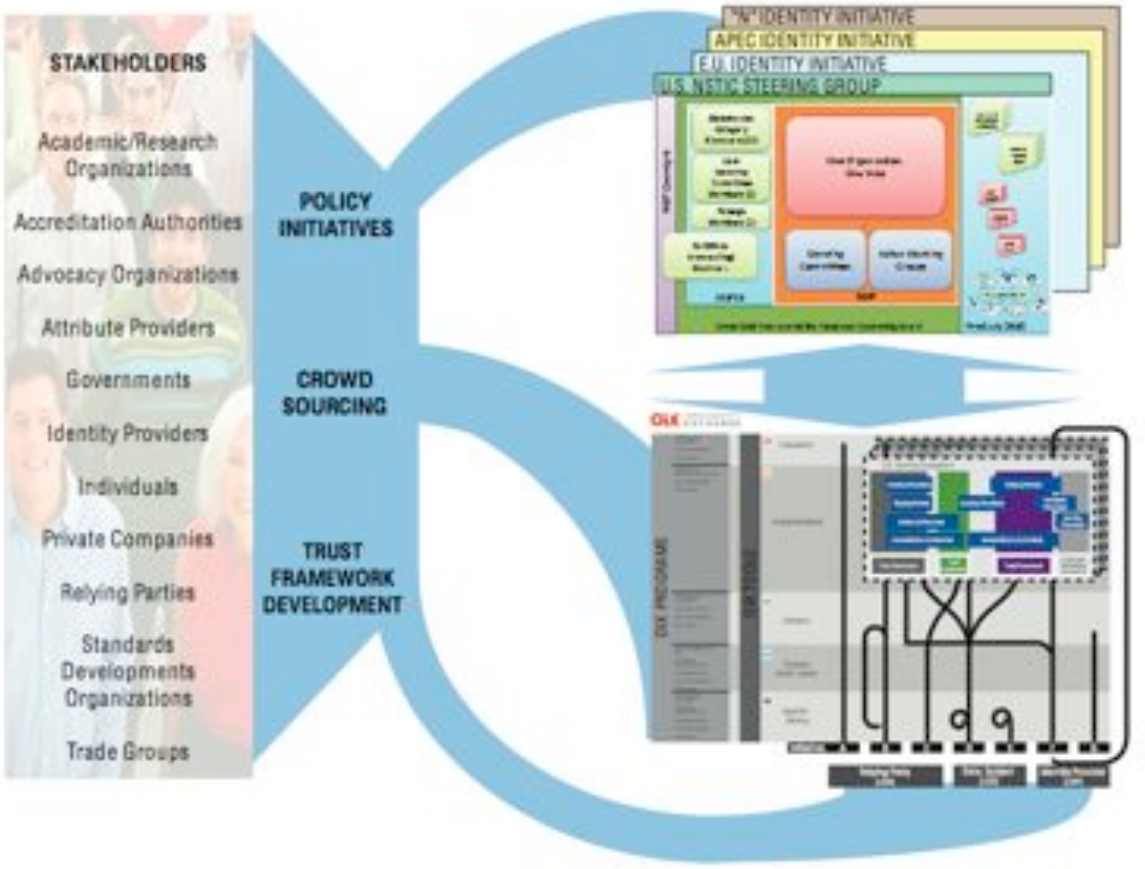
Additional notes relating to Diagram:

Point 5 of the July 13 Points of Consensus reads: “Smart Grid is a sector specific, yet useful model of phased development (Stage 1: Design, Stage 2: Rules, Stage 3: Execution).” Like the Smart Grid approach, the organization of the Steering Group should be pursued in phases and participants should prepare to be flexible throughout the process.

Essential to the SGIP and SGIPGB was the designation of distinct stakeholder groups. This will be a greater challenge in the more open data/identity markets, but the identification and inclusion/representation of all discernable stakeholder groups is essential to Steering Group Governance, and must be prioritized as part of any evolving governance structure.

A clear point of distinction between the Smart Grid and the July 13 Points of Consensus is the presence of NIST oversight in the SGIP structure (as reflected in the diagram) in the steady-state. In the Identity Ecosystem, by contrast, government should play a role in the initial stages of the Steering Committee governance structure development, but in steady-state private-sector led form, government participates as a stakeholder in the Steering Group plenary.

**Diagram 5 – Pathways to Stakeholder Participation**




Purpose of Diagram:

The purpose of Diagram 5 is to illustrate how the "Pathways to Stakeholder Participation Governance Model" relates to the Identity Ecosystem rule setting processes illustrated in Diagrams 1-4. Diagram 5 also shows how the U.S. Steering Group (and the potential Steering Groups of other legal jurisdictions) plays a critical role in the Participation Governance Model.

Brief Explanation:

The Participation Governance Model is intended to provide data/identity system stakeholders with multiple opportunities to participate in the rule setting and policy processes that inform Trust Framework and Ecosystem Framework development. Parties can participate by working with private Trust Framework initiatives (the bottom most path in the diagram), or by directly interacting with Trust Framework development and related materials via OIX tools and programs (the middle path in the diagram), or by participating in a Steering Group as a member or a participant in Steering Group-run subcommittees, programs and meetings (the top path in the diagram). OIX tools and programs support each of these pathways to participation, and through their use, encourage collaboration and interoperability among different Trust Frameworks.

The first two pathways were illustrated in Diagram 3. The third pathway, i.e., through the Steering Group, is introduced in this Diagram 5.

Tour of the Diagram:

On the left of Diagram 5 is the pool of all stakeholders including individuals and legal entities (whether commercial, governmental or otherwise) that use networked information systems worldwide. Also included are various organizations such as standards development organizations and non-governmental organizations, which currently play a significant role in international standard setting. This broad range of "entities with legal capacity/rights" is included because the rules that are the subject of the Trust Framework Development exercise are potentially relevant to all such legal persons (individuals, legal entities and governments, etc.) all of which can benefit from the normalizing and risk reduction benefits of uniform rules to legal persons that use data and/or the identity integrity management services that are provided online. This is true whether they are using networked information systems in a B2B, B2C, B2G, G2C, C2C or other contexts.

The SDOs and other entities involved in rules development are included, not because they will benefit from more reliable data/identity systems (although they will), but because their work, particularly with respect to technical aspects of these systems, is instrumental to the future success of these systems, and can be leveraged by the Steering Group through the Participation Governance Model.

Pathways to participation:
NSTIC confirms that stakeholders are never forced to participate in the Identity Ecosystem. Participation is voluntary both in the decision of whether to use the systems that are made available, and whether to participate in their development.

For those legal persons that choose to participate in development, at least three pathways to participation are provided in the Participation Governance Model as illustrated in the diagram (see pathways leading from the pool of stakeholders in the left side of the diagram). These are:

1. As a participant or commenter to a particular Trust Framework development initiative,

2. As a person accessing and commenting through the publicly available OIX knowledge center wiki or other OIX online tools, and

3. Through participation on the Steering Group as a member of that group, a party advising a member, or in Steering Group online or live collaboration programs and events.

These are shown as being hosted and supported by OIX programs and tools through all stages of rule development.

A reduced-size rendering of Diagram 3 occupies the lower right corner of Diagram 5. Imagine that the camera has "pulled back" from the view of Diagram 3, and is now showing the structure that supports the Trust Framework development illustrated in Diagram 3, the destination of one pathway to participation.

In the upper right, Steering Group straw man from Diagram 4 comes into the picture, as yet another destination for participation, while entertaining the possibility that there will be more than one steering committee, each representing a sovereign jurisdiction (such as the U.S.) or a subdivision thereof (such as a province or state), or combinations of sovereigns (such as the EU or APEC) and/or subdivisions.

These Steering Groups are shown in the diagram in two roles. First, they represent a potential pathway for participation to the stakeholders in the Identity Ecosystem. Second, the Steering Groups will themselves be participants in the work of supporting Trust Framework development in an open market in a manner that encourages participation and adoption of the Identity Ecosystem Framework promoted by each such Steering Group. In this regard, it is presumed that for every Identity Ecosystem shown in Diagram 3 (behind the U.S. Identity Ecosystem box), there will be a corresponding Steering Group that will help to promote its adoption.

In the proposed model, it is anticipated that other jurisdictions, representing other legal, social, political and cultural traditions, may wish to also form Steering Groups to represent their current interests. This sets up the possibility of being able to foster interaction *among* Steering Groups (each representing different jurisdictions, cultural traditions, or combinations of the same, e.g., there might both an EU Steering Group and a German Steering Group formed) in the future to promote the identification and standardization of common system features and requirements across jurisdictional silos. This interaction in would be an extension of the NSTIC strategy to do the same across sectoral silos (such as healthcare, financial, retail, governmental, social, etc.).

Of course, merely setting up separate Steering Groups to promote separate Identity Ecosystem Framework does nothing to promote interoperability across jurisdictions. In order to achieve that desirable result, it is necessary to create communication across and among current jurisdictional silos (system to system "cross-talk"). Toward that end, the diagram illustrates that the Steering Group(s) will have access to OIX programs and tools, like each of the Trust Framework development initiatives and each of the individual stakeholders.

The use of common tools and a common platform for development work and for listing Trust Frameworks helps to support the emergence of a virtual standard setting organization that can start to effectively engage in the work of legal standardization at Internet scale. In addition, the diagram shows how OIX can act as a liaison with each of the Steering Groups to make sure that OIX programs and tools are adequately addressing the needs of each such Steering Group and the respective jurisdictions from which they arise.

Note that, just like Stakeholders and Trust Framework development initiatives, Steering Groups can also get involved through use of OIX programs and tools in any stage of rule making. A suggestion for how the Steering Group can get involved is illustrated in Diagrams 7 and 8.

<u>Additional notes relating to Diagram:</u>

The Pathways to Participation Model:

The latter diagrams (see Diagrams 5-8) illustrate the multiple pathways to participation in rulemaking that are available in the Participation Governance Model. By providing multiple "pathways to participation," substantial pressure is taken off of the Steering Group itself in terms of Group composition, Group information infrastructure, Group access to market and stakeholder views and information, Group deliverables, etc.). This support structure in which the Steering Group can be embedded helps to preserve Steering Group resources and attention for important "best practices" review work, standards development, and finalization, as well as a proposed collaboration role to be made available to Trust Framework development efforts (see Diagram 8).

As examples of current "pathways to participation," anyone with access to the Internet[12] can go up today to the OIX website and make entries in the Knowledge Center Wiki to convey their thoughts and views about any one of the thousands of particular issues associated with data transfers and identity systems. The issues that may be raised may involve privacy, security, liability, risk allocation, interoperability, civil rights issues, user interfaces, and a host of other issues. Anyone from the public can also comment on others' ideas and even on Trust Frameworks and the formal rules upon which they are built. They can offer critique and constructive advice on how to improve the current offerings. The wiki resource is intended to collect and organize this large and growing "discussion" to help inform policy makers in both the private and public sectors. It is coupled with the market mechanism of the OIX listing service, to provide feedback to developers of Tools and Rules for future standards in the form of Trust Frameworks and Steering Group Identity Ecosystem standards.

In the alternative, the more ambitious individuals and entities can form a Trust Framework working group (as part of the OIX working group community or outside of it) and start an new initiative to promote the realization of a more comprehensive set of rules to address a current stakeholder need (or multiple stakeholder needs). Each Trust Framework initiative makes its own rules about how individuals and entities can participate in their standards setting efforts, each of which provides yet another potential pathway to participation.

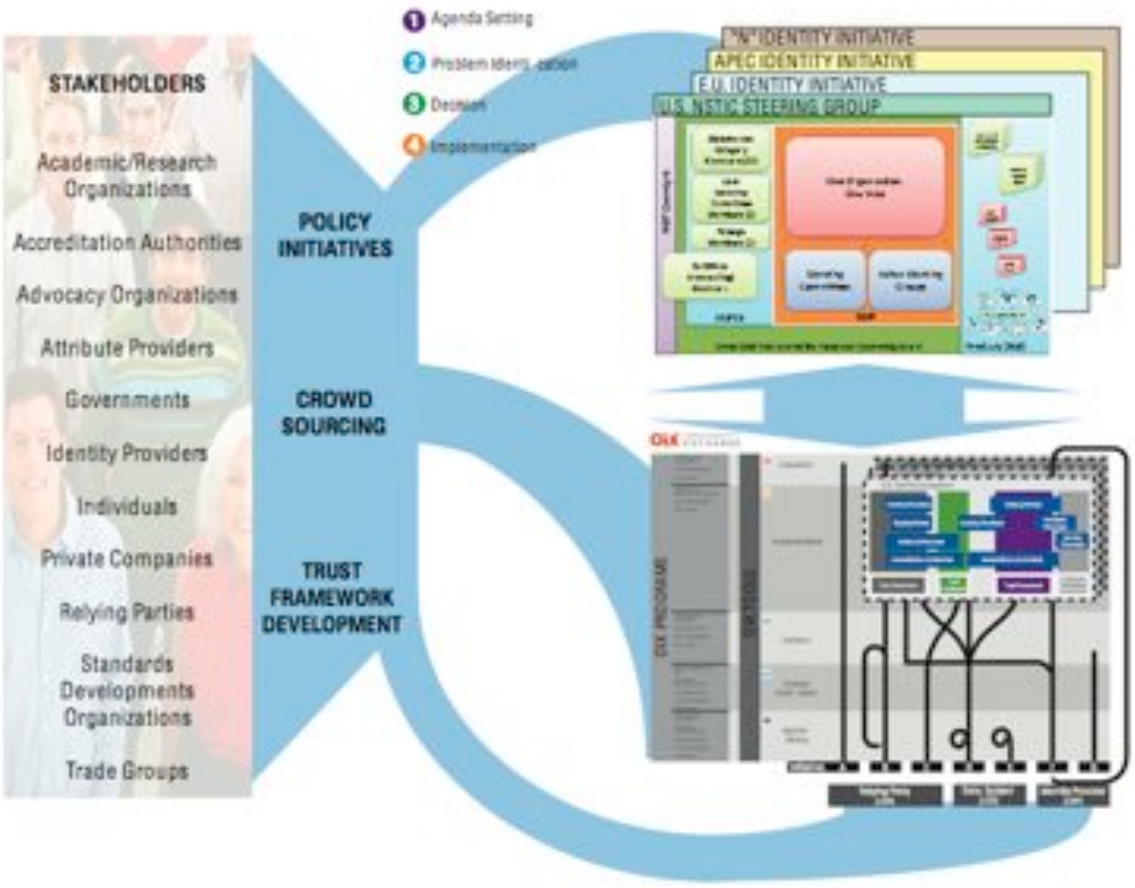
In light of the public access through the OIX tools, the opportunities to engage in Trust Framework development either as a promoter of a Trust Framework or as a participant in one or more Trust Framework development initiatives, direct participation in the Steering Group is just another way to participate. People can influence the markets today, and will have an additional vector of access tomorrow through the Steering Group.

For anyone who has an interest in how online data and identity services are developed and deployed, participation in Trust Framework rule making is not a luxury, it is a responsibility.[13] With all of the opportunities to participate in the improvement of online data/identity systems, there is no good excuse for merely complaining about systems. It is like the "camp cook rule;" if you don't like the beans, take charge and get cooking a better recipe. If you aren't willing to cook, you may get stuck eating the beans that get served. The Participation Governance Model is intended to make it easy for anyone to participate in how these systems are designed, developed and deployed and how they are dynamically modified to accommodate future change. The barriers to participation are kept low to encourage maximum participation.

[12] One common issue that all online systems encounter is the "digital divide" issue. Participation in the development of online systems is available to those with access to the technology that enables interaction with web sties, wikis and the like. The current installed base of cell phones reaches about two-thirds of the earth's population. As the value of networked information systems increases to all people, attention to the interests of the underrepresented, and strategies for bringing them the benefits of these systems, is a critical element of how these systems should be designed. This is particularly important from the perspective of whether a right to information begins to be considered as a newly identified fundamental right of some sort.

[13] This concept goes back at least as far as Plato's concept that a civically engaged citizen is a public resource, and that civic engagement is the highest form of personal freedom.

**Diagram 6 – Steering Group Initiation**




Purpose of Diagram:
Diagram 6 introduces the idea that Steering Group initiation can itself be seen as an iteration of a separate rulemaking activity.

Brief Explanation:
In Diagram 6, the now familiar five (5) stages of rulemaking are overlaid in a new place on the diagram, with the formation of the Steering Group representing the "implementation" phase of that effort.

Because the "implementation" phase is preceded by the "agenda setting," "problem identification," and "decision," phases, these are also marked on the diagram. It is recommended that the Steering Group initiation activity apply this construct to generally guide the effort to stand up the Steering Group. This approach accords with the July 13 Points of Consensus, which also call for a "phased" approach to Steering Group initiation.

In an effort to accelerate that process, Exhibit 6A to this document provides a copy of the Smart Grid Interoperability Panel (SGIP) and SGIP Governance Board charter, marked to indicate initial suggested changes needed to make that document useful as an initial discussion draft of a potential Steering Group charter.

Tour of the Diagram:

Diagram 6 is the same as diagram 5, except that it also shows the process of development of the Steering Group in its own 5 stages rulemaking process. The creation of a governance structure is a type of rulemaking, even though the work of the resulting Steering Group will be engaged in further rulemaking.

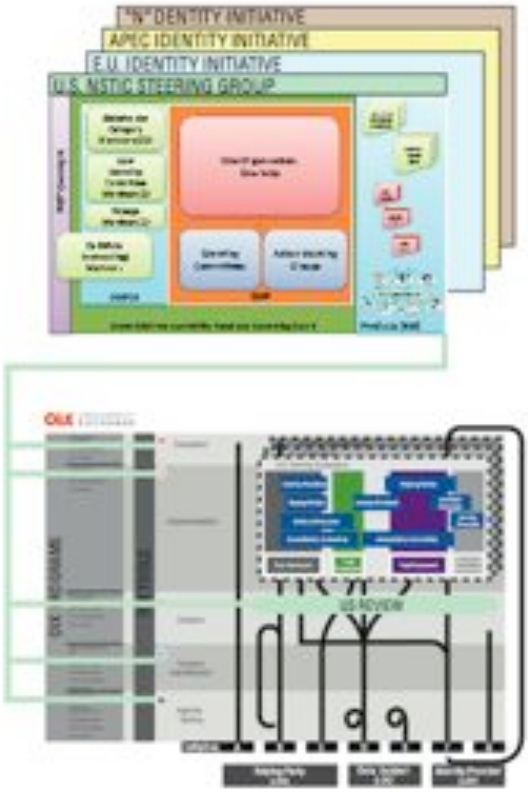
Activities during the agenda setting stage of Steering Group governance rulemaking include the NIST workshop held in Washington D.C. on June 9-10, 2011 at which governance issues were discussed.

It has been suggested that a group be constituted to spearhead construction of the Steering Group and take it from the current agenda setting stage through "problem identification," and "decision," to full "implementation." That effort was kicked off in the D.C. governance workshop, continued in the July 13 D.C. meeting of various SDOs and other parties, and is continuing in the ongoing discussions among private sector representatives who, in seeking to coordinate efforts to respond to the NOI, are simultaneously engaging in the "agenda setting" and "problem identification" processes that precede "decision."

OIX went through a similar process of establishing governance rules when it put together its rules for creating programs to support Trust Framework development processes in both premarket and open market settings. The Trust Framework initiatives that use OIX tools and programs are engaged in yet another rule setting activity.

The presentation of the draft charter is intended to help jumpstart the process to describe a potential "decision" that can help clarify the current processes of "agenda setting" and "problem identification" that was furthered in the recent workshop. The draft charter does not reflect OIX views on how the Steering Group should be governed, but is provided as a "trial balloon" for critique and improvement.

**Diagram 7 – U.S. Steering Group Role in the Identity Ecosystem**




Purpose of Diagram:
Diagram 8 illustrates how the Steering Group can use OIX programs and tools to achieve its information and standardization goals in the open market of Trust Framework initiatives.

Brief Explanation:
As noted above, the Steering Group(s) can interact with OIX programs and tools to gather information on Trust Framework market trends and specifics of Trust Frameworks that are listed or under development in order to inform its deliberations on potential candidates for Rules and Tools standardization at the Identity Ecosystem level. This helps the Steering Group to *receive* relevant information.

The Participation Governance Model also provides an avenue for the Steering Group to *convey* information to the broader market. This can be done in several ways. First, the Steering Group can, like any other party, post materials to the OIX Knowledge Center Wiki. Second, and more importantly, it can use the online OIX online collaboration tools to reach out to Trust Framework development initiatives in the data/identity markets to provide them with advice on whether their respective Trust Frameworks "line up" with the requirements of their respective Identity Ecosystem Frameworks.

In the earlier period, that "reaching out" interaction is likely to be more informational. As specific Identity Ecosystem Framework standards are developed, that interaction may become more normative, i.e., the Steering Group may choose to establish a certification process and trustmark scheme against which Trust Frameworks can volunteer to have their respective offerings tested. That will not be possible until the Steering Group first establishes some standards against which systems can be tested.

Tour of the Diagram:

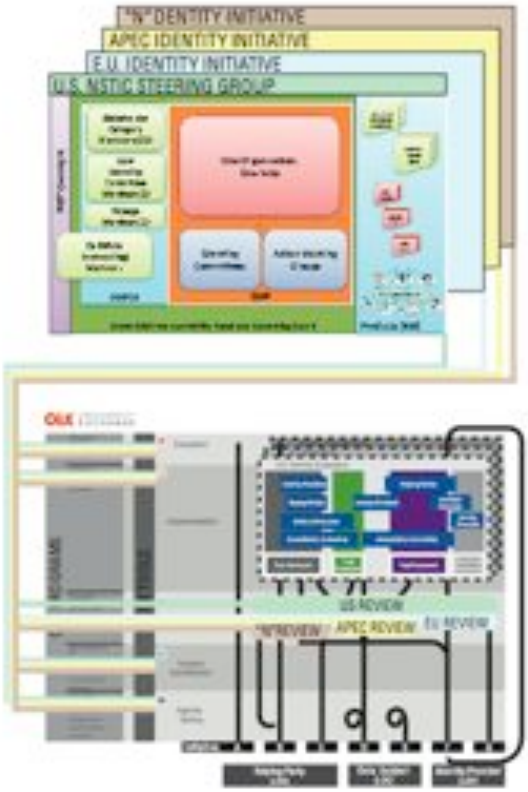
Diagram 7 is a "close up" of the right half of Diagram 6. It shows how Steering Groups can use OIX programs and tools to "communicate" with the market and with specific Trust Framework development initiatives. Communication is necessary to bring separate systems together. Effective communication is two-way, i.e., receipt of information and conveyance of information.

The Diagram indicates that the Steering Group(s) will have access to OIX tools and programs to provide information relevant to their work. That helps support their receipt of market relevant information from which legal "best practices" can be identified as candidates for future legal and policy standardization. The diagram illustrates that a Steering Group can participate and provide guidance at any stage of the development of one or more Trust Frameworks (at the invitation of a Trust Framework, or by unilaterally posting comments to the OIX wiki).

The diagram also illustrates how, at or before the "decision" stage, when an individual Trust Framework is finalized prior to implementation, one or more Steering Groups can offer to review and comment on the conformity of a draft Trust Framework to their Steering Group standards.

The review is voluntary, and the benefit of the review is the ability to assert conformity with the U.S. NSTIC standards. Conceptually, this Steering Group review service/certification process is akin to review by a technical committee or interoperability committee (or other intermediate review level) of the work of a particular working group in the context of technical standards setting. In the technical standards setting, such committees either approve draft standards or provide comments, sending the draft standard back to the relevant working group for further work.

**Diagram 8 – International Application of the Participation Governance Model**




Purpose of Diagram:
Diagram 8 illustrates how multiple Steering Groups arising in different jurisdictions can interact in the overall data/identity markets to provide voluntary review of Trust Frameworks in development to encourage their alignment with local and international standards.

Brief Explanation:
Diagram 8 illustrates how different Steering Groups, representing different jurisdictions and/or cultural traditions can operate simultaneously to provide private Trust Frameworks under development by different Trust Framework initiatives with the option to seek advice and/or certification of conformity with one or more Steering Group standards.

Those Trust Frameworks that receive the broadest range of certifications will be viewed in the data/identity markets as the ones that have achieved greatest interoperability across jurisdictions on the "rules" level, and which therefore can support access to the broadest range of markets, and the greatest certainty against "risks" of privacy and security transgressions and offer the greatest mitigation of potential liability.

Tour of the Diagram:

Diagram 8 is similar to diagram 7 except that multiple Steering Groups are simultaneously offering to review/certify various Trust Frameworks in development. This interaction is shown as occurring at the "decision" stage of rule setting when the various Trust Framework proposals are sufficiently developed to be reviewed.

This does not preclude one or more Steering Group(s) from also offering programs at other rule setting stages (such as "problem identification") in order to encourage greater interaction with, and influence over, different Trust Frameworks.

# PART I EXHIBITS

## 2A: Detailed Discussion of Rule Setting Steps

This exhibit provides an extended discussion of the five (5) generic stages of rule setting as described in policy sciences literature.[14] The characteristics of each phase vary from one rule setting context to another. Thus, for example variables such as the proportion of private and governmental influence, the time spent in a particular stage, the degree of public involvement and other factors can vary from one stage to another within a given rule setting context, and from one rule setting initiative to another.

Why is attention to the 5 stages of rule setting valuable in the Participation Governance Model?

The 5 stages are intended to capture general processes that describe all rule setting contexts. In the case of the Participation Governance Model, there are at least three (3) separate contexts in which rule setting activities will be engaged in as prerequisites to the achievement of the Identity Ecosystem. These are rule setting associated with Trust Framework development, separate rule setting relating to Steering Group governance during "initiation," and rule setting work toward Steering Group Identity Ecosystem Framework development.

The first, "Trust Framework development" will be engaged in by groups within the "Trust Community" that initiates a Trust Framework development project. Several of these are underway at OIX through its working group structure. Outside of OIX, In Common, SAFE Biopharma , and TSCP are examples of Trust Framework development initiatives. Each one will go through the 5 stages of rulemaking (whether or not stated explicitly or not) to create and update their respective Trust Frameworks. The various paths of multiple Trust Framework development within the broader market are illustrated hypothetically in Diagram 3.

A separate 5-stage rulemaking process will take place in the process of putting together a governance structure during Steering Group initiation. In this latter case, the "rules" being made will constitute the governance structure and operating rules of the Steering Group. As is typical of a rulemaking process that is still in the agenda setting and problem identification stage, the "leadership" of the rulemaking process is still unclear. The U.S. federal government's suggestions that it will be involved in these early stages of Steering Group formation, but will not be directly involved in its operation is consistent with the notion described above that the proportion of public and private involvement in rulemaking can vary from one stage to another. In the present case, the government plans to be involved in the early stages in an effort to help "jump start" the process, but will end its direct involvement as the Steering Group achieves organization in order to fulfill the NSTIC goal that the Steering Group be privately led.

[14] See Porter and Ronit, *infra*

In an effort to help "grease the skids" to institute the Steering Group by the end of calendar year 2011, OIX has produced a draft Steering Group charter based on the existing Smart Grid Interoperability Panel (SGIP) and SGIP Governance Board (SGIPGB) Charter (referred to herein as the "SGIP Charter"), marked to indicate changes from the original Version 1.3 dated June 10, 2011, so that changes can be easily referenced. That redline discussion draft can be found at APPENDIX C. The intention of providing this preliminary discussion draft is to provide a focus on a potential document that can help to move the rule setting process from current "agenda creation" and "problem identification" to "decision" more rapidly. It is also intended to demonstrate the commitment of the Participation Government Model to standardization, in this case *standardization* of governance models, and to set up the possibility of standardization of some subset of governance structures across multiple Steering Groups, each representing the initiative of a different sovereign jurisdiction (or coalition thereof as in the case of the European Union or Asia-Pacific Economic Cooperation (APEC).

In the case of non-U.S. Steering Groups, the participants and governmental entity/entities will each independently decide how much that Steering Group reflects governmental or private interests, with some being wholly private, some being wholly governmental and the remainder relying on some combination of governmental and private representation on their respective Steering Group. The latter standardization across multiple Steering Groups is intended to foster greater coordination between and among jurisdictions in the establishment of their respective Identity Ecosystem Frameworks (representing their respective legal, cultural, social, political and economic traditions) with the intention of thereby fostering greater interoperability across the Internet subsystems over which they currently exercise some degree of control. This will help to address and ultimately potentially resolve issues such as the EU "safe harbor" and various governmental limitations on Internet access and use.

Finally, a third instance of rule setting will take place under the guidance of the Steering Group Identity Ecosystem Framework development itself. Once the Steering Group is formed, it will engage in activities associated with the creation and updating of an Identity Ecosystem Framework. That will include identifying and aggregating a set of policy and legal standards that will, in effect, be *rules* at the upper levels of the identity rules "stack." That means that the Steering Group will itself engage in rule setting, which will again invoke the 5 rule setting stages.

The Steering Group will need to make decisions about how groups outside of the Group itself will be involved in such rule setting at each of the 5 stages. It is assumed that the Group will seek to involve broad sections of the stakeholder community in that rule setting activity at each of the stages, but it may have different programs through which that involvement takes place to maximize the quality (and to address the quantity) of input at each stage. Thus, for example, it may run public workshops to solicit stakeholder views in early stages; use online functionality (such as that provided by OIX) to gather, focus and render persistent and accessible stakeholder analyses of potential rules standards candidates during the "decision" stage, and engage in other tailored other programs. The inevitability of public involvement in the Steering Group process provides a third potential participation point in the Participation Governance Model.

The elaboration of the stages of rule setting is not intended to establish rigid and fixed processes on the activities, but to provide a sense of the typical phases of activity that are likely to characterize every rule setting context. Awareness of these stages can help to clarify shifts in agenda, to identify resource needs at each stage, and to help parse issues that are on different tracks in the process.

## I. Stage 1 - Agenda Setting

**Q: What is stage 1 – agenda setting?**

A: Agenda setting is the first stage where different groups raise issues in related areas and where different groups identify and explore conflicts with other groups.

Discussion: The agenda setting context has a high "noise" to "signal" ratio, since at this stage there is not yet any narrowing of the issues which takes place in stage 2 – "problem identification." It is necessary to engage in agenda setting in order to "scope out" the issues, and to increase awareness of various related issues that may be impacted by the rule setting exercise.

Since it is a new area, and one that is attracting increasing attention as the value propositions associated with data/identity markets mature, it is fair to say that a substantial part of the current data/identity discussion is currently at the agenda setting process. This is consistent with the literature and, rather than being a condition to be lamented, helps to focus attention on the important function of agenda setting as a sort of "crowd sourced" brainstorming from which issues and ideas are extracted to be moved to the increasingly focused stages of "problem identification" and "decision."

**Q: Will "agenda setting" be a public or private process?**

A: As evidenced by the multiples parties involved in various aspects of the Participation Governance Model, successful agenda setting for data/identity rules will be a hybrid of public and private processes. For maximum efficiency and to enable greatest stakeholder participation, the different rule setting processes should be loosely coupled into separate but coordinated efforts. OIX tools and programs enable that coupling to occur.

Discussion: During the first stage, agenda setting, there is typically a question of whether the development of issues is best accomplished in public or private setting. For efficiency gains, there is often a preference for private agenda setting, since it has a better "signal to noise ratio." That approach is characteristic of traditional self-regulation in the context of law, medicine, insurance, the chemical industry, and other rule setting. More private agenda setting can be appropriate in the data/identity space where, for example, there are numerous "closed systems" Trust Frameworks that, because of narrower sets of users, and a B2B context can be developed privately. These include various Trust Frameworks currently established to serve the needs of the pharmaceutical industry and military equipment manufacturers. It also characterizes some B2C contexts such as PCI-DSS (and other standardized legal structures that are applied as part of the infrastructure of the payment card legal/Trust Framework).

In the case of emerging data/identity markets, particularly those that rely on the "feed stock" of so called "Personal Information" (as various defined), there is a shared interest in the area by the general public, businesses and government authorities, so that a hybrid private/public agenda setting process is appropriate, and any inefficiencies associated with more broadly public processes will need to be re-gained through other process decisions.

Since it has a strong public component, success will go to the market participants that can help provide solutions to public concerns. At present, those concerns are, however, incompletely defined, and so the

exercise may be as much about expectation setting as anything else. In any event, given that the nature of the discussion is of interest to the public from many angles, more public rule setting processes are more appropriate, particularly for consumer facing products and services.

The NSTIC workshops are an example of how the U.S. government is sensitive to these issues, and is attempting to engage the public in the early "agenda setting" process both with respect to the rule setting associated with Steering Group Governance (through the DC governance workshop) and the separate rule setting associated with Identity Ecosystem Framework creation (through the Boston and later West Coast workshops).

## II. Stage 2 - Problem Identification

**Q: What takes place at stage 2 – problem identification?**

A: Problem identification is the stage where issues raised during "agenda setting" are narrowed to those that lend themselves to the crafting of rules and solutions in stage 3 – Decision.

**Q: How can the Participation Governance Model and OIX tools and programs help in the transition from agenda setting to problem identification?**

A: The Participation Governance Model and OIX tools can enable greater awareness of the stages of rules development that can help the parties to "liberate" issues from the discussion stage to the action stage by collectively recognizing when issues are "ripe" for the transition.

Discussion: The transition of one or more issues from agenda setting to problem identification can be affected by a number of factors including political and other non-substantive considerations. As a result, it can be a difficult transition that can be substantially delayed, which prevents the advancement of the process of seeking to narrow the focus onto problems that lend themselves to being addressed in later subsequent rules creation steps that occurs in problem identification.

Where technical, administrative or other "back office" issues are involved (including those issues that are not expected to attract enhanced scrutiny from any stakeholder group or otherwise be controversial), the transition can often occur more smoothly and efficiently from agenda setting to problem identification. To the extent that such issues can be advanced through to decision and implementation, the rules that they generate can provide a helpful foundation for working through rules-based solutions for the more difficult and controversial problems.

For example, the advancement of legal standards for the more mechanical aspects of levels of assurance (which are dependent on measurable processes intended to reduce credential entropy through identification, proofing and authentication exercises) will help to provide a more reliable foundation for the exploration of appropriate solutions for various challenging and sometimes controversial issues currently grouped under the rubric of "security" and "privacy."

Of course, in some cases the issues will be more tightly coupled, requiring that they be advanced through the rule setting process in a more coordinated fashion. For example, where, such as here, there are data subject LOC (a.k.a. "levels of control" or "Privacy") related issues of interest to both governmental, individual and commercial (e.g., small business) stakeholders, and where normalization/resolution of the types of issues that could compose a mature LOC metric is ultimately dependent on resolution of such user-centric issues, it may be necessary to both consider the issues in a coordinated fashion and may also be desirable to split issues to separately work on those that are more technical and/or can be dealt with in smaller sub-groups at the problem identification stage.

The OIX working groups structure was designed to allow the easy separation and customized coupling of issues/discussions into groups and subgroups as needed to foster efficient, transparent and participatory development, and can thus serve as a valuable resource to the Steering Group.

Each OIX working group is separate, can determine its own Intellectual Property Rights (IPR) and governance policy, and is able to proceed on its own work plan and at its own pace. Some WGs may be more comprehensive (such as one that works on a national level Trust Framework to match the broad requirements of a given Steering Group's Identity Ecosystem Framework), while others may be more narrowly focused (such as an LOA-only framework, an LOC-only framework, an LOP- only framework (involving relying party best practices (RP-BP)), etc.).

**Q: How else can the Participation Governance Model help during the problem identification stage?**

A: The Participation Governance Model, working at Internet scale, will engender more comprehensive standards for selecting the issues to make the jump from agenda setting to problem identification, all while keeping with the requirements of Internet scale for configuring normalized Internet scale data/identity systems.

Discussion: Traditional rule setting confined to countries or limited sets of countries will likely result in the perpetuation of jurisdictional silos. This will raise compliance costs for data/identity service providers and other stakeholders across multiple jurisdictions. Policy is needed here at the international level. Quite simply, public (governmental) policy making is state bound; it is limited to a single jurisdiction and is rarely international (except in the case of some NGOs (non-governmental organizations and treaties)). This is an Internet scale effort, and thus an application for the Participation Governance Model.

In addition, even within jurisdictions, industry policy can cause data/identity solutions to be siloed due to regulatory constraints and historical industry competitive patterns. Thus, health care, telecommunications, financial and retail-based data/identity systems are still largely separated due to their respective organizational artifacts of earlier external pressures in their previously separate ecosystems.

It is typically difficult to do policy across industries and jurisdictions. However, a Participation Governance Model using common tools and programs can leverage the reach of the discussion to allow policy transfer across jurisdictions, industries and territories, and so can achieve interoperability more readily by leaping over hurdles.

It is because Data/identity services play an increasingly important role in many industries that these bridges are available. The providers of those services, which are heavily represented on the OIX board

and membership, are in a good position to be the agents of interoperability, given the reach of the data/identity infrastructure that they collectively represent. The Participation Governance Model is intended to enable the participation of the broad group of data/identity stakeholders, in an effort to build more resilient, sustainable, responsive and successful data/identity products and services that together with their respective users comprise the Identity Ecosystem.

**Q: How is OIX set up to help make the difficult transition from agenda setting to problem identification easier?**

A: OIX tools and the working group structure are intended to foster the Participation Governance Model to help stakeholders to separate the "wheat from the chaff" as issues are winnowed from the broader discussions of agenda setting.

Discussion: OIX was set up specifically to make private rule setting easier; to support the rapid and responsive normalization of the data/identity markets. The Agenda setting process (the first stage) can be conceived of as relatively disordered with swirling and interrelated issues arising from social agenda, commercial agenda, governmental agenda, civil rights agenda, consumer protection agenda, etc. All of these important issues, and others, are mixed together at the agenda setting stage.

The second stage exercise of "problem identification" can be thought of as the capturing and specification of issues/problems "signal" from the "noise" of agenda setting. The successful transition represents an improvement in the "signal to noise ratio" of the relevant issues to enable the making of decisions in the following stage 3 – "decision."

The transition from agenda setting to problem identification can be visualized as a pachinko machine; balls are released and bounce somewhat randomly off a series of pins, but eventually land in individual slots at the bottom of a pachinko machine. The pins are the agenda setting process; the slots are the problem identification process. Note that all the balls ultimately find their way into slots in the machine, just as all agenda issues can ultimately be accounted for in problem identification. In other words, the improvement of the "signal to noise" ratio does not require that any stakeholder agenda items be ignored or abandoned, only that they be coordinated with other issues into their own problem identification "slots."

Notably, where the rulemaking at issue is private Trust Framework development (see Diagram 3), all decisions on advancement from one stage to another are made by the trust community that is developing a particular Trust Framework. The stakeholders involved in that trust community have total discretion to establish governance and "legal standards advancement" processes and criteria to suit their respective needs. Where those Trust Frameworks are being developed within the OIX working groups community, the OIX board approves working group charters, but after that, all Working Groups proceed independently, supported by OIX tools and programs, but making their own development and finalization decisions. Where the Trust Frameworks are being developed outside of the OIX working Group community, the only limitation on Trust Framework organization and operation is relevant local law.

The OIX working group structure and its relationship to the larger Participation Governance Model was set up to accommodate the "energy" associated with agenda setting, while encouraging the refinement of issues needed to move through problem identification and other later stages of rule making. In short, the OIX processes and structure, and the preparation of the Knowledge Center materials and related

tools provides a useful "landing strip" for the issues that can help to guide the transition from agenda setting to problem identification all within the discretion of each trust community developing a Trust Framework.

That latter point is the reason that OIX has prepared the redlined version of the Smart Grid Charter as an initial discussion draft of a potential Steering Group charter. The draft is intended to provide a preliminary "landing strip" for issues from agenda setting. OIX does not advocate for the finalization of the Steering Group Charter based on the form of this initial redlined draft, but intends through its preparation to provide a platform for the discussion of Steering Group organization and operation.

**Q: How can the operation of the Participation Governance model at the "problem identification stage" help to address consumer/citizen issues efficiently and transparently?**

A: By providing an overall framework for stakeholder engagement, a Participation Governance Model and its related subsidiary rule setting processes can help to promote individual participation, and can enhance the quantity, variety and quality of communication channels made available to individual participants who might not otherwise have a voice in the rules discussions that will affect them. The model also provides an overall structure for larger data/identity markets through which stakeholders, including individuals, speak through their data/identity product and service consumption decisions.[15]

Discussion: The involvement of individual data/identity system stakeholders in the early stages of rule setting processes, i.e., the Trust Framework and Ecosystem Framework development processes, is extremely valuable, but is substantially more complex to accomplish in practice, since the sheer numbers of people (and views) are very large making it more difficult to process the "views" and understand the "needs" of the group.

Mechanisms to gauge group needs typically involve either voting (to make a single group decision) or market mechanisms (to make multiple simultaneous group decisions).[16] The Participation Governance Model is intended to support both approaches, anticipating that stakeholders "vote" as participants in individual Trust Framework development activities, and participate in normalized "markets" as producers and consumers of data/identity products and services that are standardized through operation of the overall model. The Participation Governance Model can help to develop markets that provide "voices" to large groups and the individuals and other stakeholders of which they are composed.

Because involvement of system "users" (data subjects and relying parties) early in the decision process (such as agenda setting and problem identification), can help make a rule setting process within the Participation Governance Model more effective and legitimate, OIX is designed to accommodate that involvement.

---

[15] Conversely, but confirming the relationship of consumer preferences and markets, it has been asserted that to the extent that a relevant factor affects consumptive behavior in the data/identity markets, it may help to define new markets. *See* "Privacy in Antitrust: A Relevant Product Market Factor," Pamela Jones Harbour and Tara Isa Koslov (in the Bureau of National Affairs, Inc. Privacy and Security Law Report (Feb. 28, 2011)(asserting that to the extent that the notion of "privacy" affects consumer decisions, it is a relevant factor in market definition.).

[16] See Part VII "Institutions and Aggregate Behavior" in Networks, Crowds and Markets (Easley and Kleinberg), *supra.*

Toward this end, the OIX working group structure was designed to be flexible to accommodate various governance structures that may be employed to encourage participation of large user groups, such as alternative voting mechanisms, rules comment functions and the like.

**Q: During the problem identification stage, how are problems identified and selected as the focus for development of rules, and how are "best practices" discerned and documented?**

A: While objective criteria are very strongly preferred, there are many other possible influences on the problem identification stage that have been evidenced in other various rule setting initiatives. As a result, there is evidence that participants that are involved in configuring the processes may sometimes have a potentially greater impact on the results. These are human institutions that will continue to be affected by various human factors. The transparency and access that is encouraged by the Participation Governance Model is intended to help make these influences more explicit so that they can be known and addressed.

Discussion: It is important to apply objective, clear criteria during the problem identification stage. Not surprisingly, however, the process is not always entirely neutral.

In addition to objective criteria, the identification of issues for rules development also involves considerations such as: the nature of prior rules (legacy), the interest of existing authority structures in incrementalism (bureaucratic inertia), resource constraints (cost considerations), and a variety of other political, cultural, social, technical and practical considerations. At Internet scale, the variety of these influences is significant. The Participation Governance Model relies heavily on market mechanisms to enable the identification of commonalities across them.

Given the variety of non-objective influences that are possible at the problem identification stage, there is an advantage in being involved in the configuration and management of the processes in order to make certain that any influences that are applied will be directed toward system and stakeholder positive goals and objectives. This is why the Participation Governance Model enables several different vectors of individual participation. For example, if an individual or group is "shut out" of a particular Trust Framework development initiative for whatever reason, they may still participate directly through use of OIX tools including the online wiki to express their views (see Diagram 5).

**Q: Why has OIX already created the online Trust Framework development toolkit?**

A: Trust Frameworks save costs, reduce risk, encourage innovation and market expansion, and offer a potential path to more comprehensively address seemingly intractable security, privacy and liability concerns. Trust Frameworks make economic sense. Unfortunately, the processes associated with "rule setting" as opposed to "technical standards setting" are relatively unfamiliar to those not already involved in related legal and policy work.

OIX recognized early on that many Trust Framework initiatives were stalled in the "agenda setting" stage, even though they had access to relatively advanced *technology* solutions with which to pursue stakeholder goals. The OIX toolkit is intended to foster easier and more deliberate transitions from one stage to the next in the rule setting process, including in particular the challenging step from "agenda setting" to "problem identification." By helping individual Trust Framework initiatives to make the

transition toward completed legal standards, OIX furthers its formal organizational purposes of improving conditions in the data/identity sectors generally.

Discussion: The online OIX toolkit is ready to host the activities associated with problem identification. It provides a "landing strip" for the agenda, like landing on an aircraft carrier in heavy (agenda setting) seas. This allows the easier extraction of issues from the agenda setting exercise.

That "extraction" exercise is pursuant to a consistent "data actions" structure that provides a uniform development platform for aligning the legal and technical considerations in the form of Trust Frameworks. The employment of a data-action-based analytical structure reflects an effort to base the analytical platform on a set of variables that all data/identity systems have in common, i.e., the handling of data. The data flow survey tool and the knowledge wiki focus on individual data actions (such as data collection, data storage, data access, data disposal, etc.) as the common variables across systems.

The power of focus on *actions* is that each action is taken by a party. The presence of that party provides a legal person to whom enforceable legal duties can be assigned to further Trust Framework goals. Those duties can further all stakeholder security, privacy and other goals. In addition, since there is no legal liability without there first being a duty, structured duties for data actors can help to address the "liability" issue by establishing more certain and objectively testable "standards of care" for data handlers reducing compliance costs and reducing or eliminating unknown risks.

The focus on data actions helps to "rationalize" the discussions of the agenda setting stage. It is the path of least resistance to operationalization of the agenda items, and is objectively presented.

**Q: During the problem identification stage, what are the variables that affect whether an "agenda item" in the first stage will be reflected as an "identified problem" at the problem identification stage?**

A: The variables that affect the decision of which issues to move from agenda setting to identity management include both objective criteria (such as severity and likelihood of harm and complexity) and subjective factors (such as the inertia of legacy rules and political considerations (noted above)).

Discussion: The most obvious variables for determining whether a problem will ascend from the "agenda setting" stage to be identified during the problem identification stage are such intrinsic considerations such as the severity and complexity of the problem, but there are also certain extrinsic considerations that come into play such as cost, commercial viability, deployment and sustainability issues and a host of others.

An example of the challenge of deployment and sustainability issues is presented by the current status of the U.S.-GSA FICAM procurement specification. It presents a "relying party" based statement of system requirements for the reliable accomplishment of credential systems based on more objective and testable LOA, but isn't yet developed into a full proposal of how those requirements can be commercially and sustainably met for commercial tools and services to continue to satisfy those relying party needs, particularly at higher levels of assurance. Those discussions are continuing.

Scalable and sustainable systems must be commercially viable (which for fundamental information network infrastructure are at Internet scale). Private development and markets are the best way to

discern and test the overall economic viability of a given structure. The question of commercial viability is critical, since it incorporates the power of market mechanisms into the development process.

These systems will be expensive to build, deploy and operate. That is the reason that FICAM, NSTIC, and the Commerce Department's privacy Green Paper all look to the private sector to carry the development load. Sustainable structures will also address how the development and building expense will be paid.

To the extent that "development and deployment costs" can be derived from the system itself to pay some of the development expenses, it will favor speedier construction.

Comprehensive, mutual contractual structures are the cheapest to build, by reason of the simple expedient that they afford the opportunity for all stakeholders (contract parties) to offer and receive from one another contract-based "compensation" (called "consideration" in contract jargon) in the form of promises, rather than money. Where those promises are to do (or refrain from doing) something that a stakeholder cares about (like protecting data from unauthorized access), it has value to the stakeholder.

In other words, an enforceable contract can be supported by the mutual exchange of promises, with no money needing to change hands. Comprehensive structures that involve multiple parties lend themselves to larger scale, simply by virtue of their ability to leverage the mutual exchange of promises of all parties to do what they promise, for fear of losing the system benefits of the other parties' mutually dependent promises.

Comprehensive Trust Frameworks are cheaper to build, since more parties' promises to perform duties in accordance with a given standard of care are available as the "contractual currency" to pay to other participants.

**Q: What are the implications of "privacy by design" as advocated by several governmental authorities with respect to the Participation Governance Model?**

A: The concept of "privacy by design" reaches deeply into private organizations to promote good data/identity "hygiene" practices. If the standards applied through "privacy by design" techniques and approaches are generated *externally* to the organizations, that "reach" might be perceived as an intrusion. The Participation Governance Model allows the stakeholders that are subject to the rules embodied by privacy by design approaches to have a say in the required standards from which those rules are derived, substantially mitigating the administrative challenges of "privacy by design."

Discussion: The concept of "privacy by design" assumes that privacy-supporting practices should be built into all aspects of commercial and governmental data-related operations that involve data about an individual. Any external implementation of privacy by design would necessarily require a deep penetration of the rules and processes by which of how businesses actually operate.

This would be similar to the impact of The Sarbanes Oxley Act,[17] but would not be limited to financial systems; it would impact all data/identity systems in business. Many companies perceived of SOX as intrusive.

[17] Sarbanes Oxley Act of 2002 (Pub. L. 107-204, 116 Stat. 745, enacted July 30, 2002).

The rules standards to guide "privacy by design" should be developed with leadership from the stakeholders that they will affect. To the extent that the concepts are being applied to commercial systems (such as those that handle data), a dialog will need to be had among commercial actors, since even customers can't always directly help to inform the rules development efforts for some aspects of business data/identity systems. Most of the requirement of privacy by design will need to be implemented in the "back office," where data is handled by businesses applying operations that may be complex and beyond the understanding or interest of customers. Reducing that complexity is one of the goals of legal standard setting.

The bottom line is that because the "legal duties" of legal entities must rely on the creation and implementation of formal rules to guide employee behavior in a cohesive and comprehensive manner to achieve company data/identity goals, businesses should be given the opportunity to provide thought leadership on internal rules relating to privacy by design standards. The Participation Governance Model enables such participation, whether by commercial, governmental or individual relying parties, identity providers or data subjects.

Stakeholder consensus processes fostered by the Participation Governance Model, led by private parties that will be subject to the rules, will provide the greatest ability of businesses to determine achievable and administrable pathways to privacy by design. It will also be advantageous to competition by establishing new markets for those businesses that offer services to other businesses (B2B) to help them implement "privacy by design," such as consulting, network, technical, legal and other services.

## III. Stage 3 - Decision Making

**Q: What is stage 3 - decision making?**

A: Decision making involves the selection of Stage 2 "problems" to address and the making of decisions and new rules of how to deal with them.

**Q: Does NSTIC seek to guide the decision making part of the process?**

A: Yes. Through its promotion of FIPPs-based legislation, NSTIC would purport to move the FIPPs approach to the LOC metric directly to "decision making," skipping or at least attenuating the discussion and debate that occurs at the agenda setting and problem identification stages.

Discussion: Yes, in part. Sometimes decisions are made before agenda setting and problem identification are complete. NSTIC, for example, indicates that fair information practice principles "must be universally and consistently adopted and applied in the Identity Ecosystem."[18] This is a strong statement that at least some form of FIPPs will be part of the government's "identity ecosystem" package.

[18] See NSTIC at Appendix A.

The assertion by government of the need for FIPPs-based solutions is a form of "decision making" that skips over the agenda setting and problem identification stages. Fortunately, there are many aspects of FIPPs that would present little or no significant administrative challenges to private parties. Traditional FIPPs needs further development if they are to be practically and commercially viable for future data/identity systems.

Further, the substance and framework of FIPPs are sufficiently broadly applied (although with varying iterations) in multiple jurisdictions, that future consensus-based versions of FIPPs could provide a very helpful platform from which to generate broadly interoperable "legal" standards for the LOC metric of Internet scale data/identity system development.

Fortunately, the U.S. Department of Commerce Green Paper suggests that an "updated" set of FIPPs is probably more appropriate as a starting point. A discussion of FIPPs development through the mechanisms of the Participation Governance Model could gainfully approach various standard rules questions from the FIPPs perspective.

For a comprehensive system such as the U.S. Identity Ecosystem, FIPPS legislation is just one leg (the LOC leg) of a three-legged stool (the other legs being LOA and LOP metrics). All stakeholder interests will need to be addressed in comprehensive solutions which suggests that promotion of FIPPS legislation without development of LOA and LOP standards will not provide a complete and sustainable solution. OIX programs are designed to give stakeholders the benefit of market information systems to help in design and deployment of such comprehensive solutions

**Q: How can the Participation Governance Model help to get us past talk and toward actions that reduce risk and liability?**

A: Application of the Participation Governance Model and the coupled rule setting processes that it supports can help provide a path from talk to action by reducing the inefficiencies associated with unclear processes.

Discussion: Agenda setting and problem identification are "talking stages." Even though problem identification is more directed toward composing rules, it is still a stage of studying and talking about risk and "how to" scenarios. Decision making is the process by which rules become actionable. As noted above, control of decision making processes is not neutral. The decisions of "how" and "when" and "what" issues to elevate to the latter steps of the rule making process matter to all stakeholders. A Participation Governance Model provides a potentially helpful "virtual organizational structure" from which to achieve a balanced perspective. Each trust community, each Steering Group and each stakeholder can pursue its particular goals through multiple participation opportunities at multiple levels.

**Q: What does a Steering Group structure, such as that anticipated in NSTIC, offer that is unique at Stage 3 – decision making.**

A: A Steering Group can lend the "tacit authority" of government to private rulemaking, effectively allowing all market participants to act as "legislators" of the rules that bind them. While Trust Framework development initiatives permit the same involvement in rule setting, at the Steering Group level, the coordination with government lends authority to the process in increments that are clear and understood by participants.

Discussion: First, no single stakeholder using Internet scale data/identity systems, whether commercial, governmental or otherwise, currently has comprehensive unilateral rule making authority. Government jurisdictional constraints limit single government action, just as online businesses rule making authority it limited to their respective Terms of Service, purchase contracts or other data/identity policy documents.

Second, the Participation Governance Model elevates all participants to the role of virtual "members of the legislature," since it provides access to mechanisms of rules creation to those parties that are affected by the rules. This is a separate form of authority that is not otherwise available to private parties. It is complementary to their current authority. The NSTIC call to the private sector to lead the effort to compose a Steering Group that will then create policy for the Identity Ecosystem Framework is an invitation to stakeholders to exercise this form of "legislative" authority.

At the decision making stage, the Participation Governance Model provides participants with ability to create rules that more appropriately lend themselves to sustainable, scalable commercial solutions. It is a chance to participate when the "rubber hits the road."

Involvement in rule setting provides stakeholders with efficacy, and systems with resiliency, sustainability and stability. In a multi-jurisdictional intangible rights regime (for data/identity rights, etc.), the realization of value and the determination of liability both depend on the presence of a normalized interaction platform guided by "the rules." If the rules are followed, stakeholders can plan. If the rules are violated, stakeholders can enforce claims to prevent and offset unanticipated liabilities (through an analysis of rules-based duties, breach, causation, damages). Whether a party is a plaintiff or a defendant, everyone benefits from clearer declarations of applicable "standards of care" for duties, so that they can stay out of "trouble," i.e., the breach and damages analysis. Would you rather draft the rules by which your liability is determined, or just respond to them?

**Q: How can OIX help to clarify the different roles for stakeholders in Stage 3 - decision making?**

A: OIX has various programs and tools to support multiple paths to Stakeholder Participation. First, the OIX working group community will support Trust Framework rules development at different stages. Each effort may involve different mixes of private and public initiative and resources. By bringing together the different efforts into a single community, it will be easier to compare the respective roles for each stage, including the critical rule making that takes place in stage 3. This will provide useful information on rules development "best practices" that can benefit all trust communities. Second, broad public access to online tools enables stakeholder participation outside of individual Trust Framework initiatives. Third, OIX programs and tools support the Steering Group processes, which will offer stakeholders additional pathways to participation.

Discussion: Various OIX programs support the Participation Governance Model. The OIX working group structure makes it easier to compare progress across and among initiatives. The OIX working group community provides the benefit of seeing how others handle various issues; and access to knowledge which is preserved to be used by others in the OIX knowledge center. There is value in being able to discern the "best approaches" from among the groups working on Trust Frameworks.

Second, Stakeholders, whether institutional or individual, can also participate in various rulemaking settings by accessing various OIX online tools and programs. For a further discussion of OIX tools and programs see www.openidentityexchange.org .

## IV. Stage 4 – Implementation

**Q: What happens during Stage 4 – implementation?**

A: During stage 4, "implementation," the focus shifts from rulemaking systems to deploying systems, which involves issues of administration, operation, and the application of incentives and penalties to coax participation and conformity to standardized, system consistent rules..

**Q: Can the Participation Governance Model help with easing implementation burdens and costs under new sets of rules set forth in Trust Frameworks and the NSTIC Identity Ecosystem Framework?**

A: Yes. Whenever new rules are implemented, they must be integrated into the management, compliance and enforcement mechanisms associated with existing (legacy) external laws and third party contractual arrangements. If private parties are involved in rule setting, they can better configure new rules to more easily integrate them with existing systems.

**Q: How can a Participation Governance Model help during the rules implementation stage?**

A: Implementation involves bringing stakeholders "on board" to participate in the deployed system. That is, in part, an educational effort as potential stakeholders are exposed to, and asked to adopt, the description of system benefits and costs. A Participation Governance Model can help to defray the educational and other deployment costs.

Discussion: Education costs can be shared, and education programs can help to develop markets.

For example, in an interoperable "ecosystem," when users "learn" about one system, they, in effect, simultaneously "learn" other interoperable systems. Learning one system thereby helps build broader markets.

Education is important where issues are technically complex. It is also beneficial for overall system security where systems are difficult for government authorities to centrally monitor and control. An educated user base can act as a "neighborhood watch" to help keep systems secure. In fact, given the "power law problem" of enforcement in systems that undergo geometric expansion (such as data/identity markets), the "neighborhood watch" aspects of security are likely to mature into a very effective compliment to increasingly challenged central control approaches to system security and reliability. Cultivation now of mechanisms to coordinate group behavior to enable such a form of "crowd sourced" auditing and assessment will likely pay significant dividends as systems rapidly expand, catching more central mechanisms off guard.

Also, education helps to drive "expectations" which can drive the direction of markets. For example, Relying Party best practices are broadly viewed as necessary to assure the integrity and security of data/identity systems at Internet scale. Evidence of their efficacy is provided by the similar rules of the payment card system[19] that provides that system with sufficient data integrity to function in the consumer credit sector of the financial sector. If Data Subjects become educated about the "system integrity" benefits to them of relying party best practices (RP-BP), education can help serve as a forcing function for the market acceptance of rules associated with RP-BP. The same is true of other system benefits such as the benefits of user-centric controls to all parties.

**Q: How can a Participation Governance Model enhance the leverage that private sector actors can apply to bring other commercial actors within the coverage of standardized rules to enhance the value to all stakeholders of the legal standardization "network effect?"**

A: Successful rules deployments can encourage "hold outs" and other private parties in related and adjacent markets to join the market defined by the common rules derived from successful Participation Governance Model processes.

Discussion: The literature suggests that participants in private rules making processes can encourage membership (particularly of reluctant larger firms), by encouraging other entities to adopt stakeholder-derived rules. Markets can move commercial players. For larger commercial players, particularly those operating at Internet scale, it may in fact be the only way that they can effectively be moved.

The GSA FICAM program is an example of the exercise of the U.S. government's buying power in an effort to jump start markets. The effort was both a procurement initiative by the General Services Administration and an example of an effort to exploit the procurement opportunity to help develop standardized "tools and rules" that may encourage a greater "force of attraction" toward a normalized set of rules dealing with identity and attribute authentication and authorization practices. As was the case with Wal-Mart's insistence on the use of RFID technology in its inventory supply chain, the government's adoption of certain standards as a purchaser affects both its direct supply chain, and also has the potential to affect the ICAM purchase decisions of other companies indirectly, but only to the extent that the proposed system is commercially viable for both system users (data subjects and relying parties) and providers.

The FICAM program was greeted with relative enthusiasm by commercial parties with respect to systems supporting credentials at LOA 1, the lowest level of assurance in that system, since such support could be offered without significant additional cost to the commercial parties involved. It was quickly revealed, however, that at higher levels of assurance, there would be additional costs involved. At those higher levels, the parameters set forth in the government's "procurement specification" were either incomplete or incompatible with various commercial approaches for those higher level credentials. This has resulted in the situation where work is still being done to design and develop more commercially viable solutions.

**Q: How can a Participation Governance Model help commercial and other private entities to take advantage of public sector enforcement mechanisms to reduce data/identity system operating costs?**

[19] https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0.

A: The standardized rules developed through the Participation Governance Model offer a more normalized structure that permits established governmental enforcement structures to more readily be applied to address data/identity system problems. This results in potential cost savings for private actors.

Discussion: Enforcement is a critical, but expensive, component of security, "privacy," and liability management. Rules that are known to not be enforced are typically not followed. Rules generated by rules setting processes within the Participation Governance Model structure can be supported by public sector enforcement capabilities.

For example, rules standards derived from a Trust Framework initiative or Steering Group process can form the basis for establishing legal "duties of care" that might be applied both in "internal" system enforcement mechanisms (such as system incentive and penalty structures, reputation systems, etc.) and in "external" enforcement contexts such as litigation, arbitration or formal regulatory proceedings. Securities and commodities market rules are a good example of the potential for integration of government enforcement authority.[20]

To the extent that such enforcement authority is applied to render the behavior of all stakeholders consistent with system rules, it will help to preserve system integrity, and reduce system operating costs.

**Q: How can a Participation Governance Model help to reduce security costs across industry sectors?**

A: The standard rules created through the work of Trust Framework or Ecosystem Framework initiatives enable stakeholders to become more familiar with systems deployed across sectors. Familiarity makes it easier to detect system aberrations that can signal privacy or security problems. Standard rules enable all stakeholders to function as a "neighborhood watch."

Discussion: Trust Frameworks and Ecosystem Frameworks enable standardization of legal rules to help support standardization of technology tools. Broad rules standardization renders the behavior of populations on networks more reliable and predictable. This enhances the ability to automatically monitor for conduct that is inconsistent with system goals. This allows the improvement of access to and automation of user dispute resolution systems.

For example, it could help to be able to automatically monitor the vast number of relying party transactions associated with an open identity system to confirm compliance with RP-BP. A similar system based on algorithms applied against standard system rules helps to automate fraud detection in the payment card systems.

Another example is broad standardization of user interfaces (UIs), that would also enable other human actors in the system to act as a kind of "neighborhood watch," since aberrational behavior (akin to

[20] U.S. Federal law provides FINRA (the Financial Industry Regulatory Authority) with enforcement authority against individuals and firms that violate its rules, with appeal being available to certain actions to the Securities and Exchange Commission or the courts..

current personal data phishing or "pretexting" in the Telecommunications "CPNI" context)[21] will be easier to detect by users when normal system behavior is standardized.

## V. Stage V - Evaluation

**Q: What happens during stage 5- evaluation?**

A: During the evaluation stage there is assessment and reporting of the activities engaged in during implementation.

**Q: How can the Participation Governance Model help with the evaluation stage?**

A: Evaluation involves both the review of prior actions and the initiation of corrective actions. Governmental rulemaking in the form of legislation or regulation does not typically anticipate being subject to rapid dynamic alteration based on effectiveness reviews. In addition, private evaluation processes are atypical simply because they are infrequently bothered with during process planning. Where the Participation Governance Model is applied, rule setting processes are made more explicit, and, the evaluation steps can be more readily formalized, making possible better evaluation, and improved process improvement, with the anticipation that private involvement makes corrective changes easier.

Discussion: Evaluation is "slippery" and is often not well planned for in public or private rulemaking planning. However, the Steering Group, as a privately-led initiative, has a significant advantage over public rulemaking when it comes to evaluation; it is typically much easier for private rulemaking initiatives to revisit and revise rules when evaluations reveal rules design errors or when circumstances, systems, technologies and stakeholder needs change that necessitate rule revisions. .

In the public law context, it usually takes a significant number of compliance challenges before a law is changed, since the change process if so laborious for legislation and regulation.

Any rules that are developed in the data/identity space, whether by governments or private parties or by the Steering Group, will be challenged by an accelerating pace of change. The Steering Group should be structured to emphasize the continuous re-evaluation of finalized Identity Ecosystem Framework rules to feed back into the agenda setting or problem identification process; and as such can make for a much more dynamic, responsive rules environment. This reduces legal lag and its inefficiencies, which reduces compliance costs of companies.

Without control of evaluation and rulemaking processes, there is no opportunity to get the feedback loop started. The bottom line is that with the anticipated accelerating pace of change, it will be increasingly important to rely on the nimbleness of the private sector for various aspects of rule setting

[21] In response to situations where unauthorized persons were contacting the phone company and receiving customer proprietary network information (CPNI) by posing as authorized persons, the FCC passed an order (FC 07-22 (2007) placing identity authentication requirements on telecommunications companies in an effort to limit the distribution of protected CPNI information.

thought leadership. The Participation Governance Model provides a mechanism for coordination of individual privately-led efforts.

**Q: What are the factors that an effective Participation Governance Model needs to survive?**

A: Efficiency, legitimacy, standards and transparency

Discussion: Ronit (1986) asserts that:

> To survive an SRO [self regulatory organization] must pay serious attention to efficiency and legitimacy factors, but also find ways to integrate standards or transparency into the strategy.

OIX programs and tools are designed and have been deployed to support the Participation Governance Model. The tools and programs have been structured for maximum transparency in organization and operations. OIX offers efficiency to participants in Trust Framework and Ecosystem Framework development initiatives in the form of a highly developed Trust Framework development tool set. Finally, legitimacy is established by nature of the membership of OIX, its links to international data/identity initiatives, and its demonstrated ability to generate programs and tools to enable Trust Frameworks and in supporting the maturation of the data/identity markets.

OIX is not just re-purposing old programs to fit current government initiatives. Instead OIX was specifically organized and is being operated to engage in this support of rules development activity at Internet scale.

## 4A: The July 13 Ten Points of Consensus

1. Government is a stakeholder, not administrator

2. Government provides seed money

3. Peer relationship among members

4. Steering Group processes will be transparent, deliberative, and open

5. Smart Grid is a sector specific, yet useful model of phased development (Stage 1: Design, Stage 2: Rules, Stage 3: Execution)

6. Conscious effort to involve privacy/consumer/end-user constituencies

7. Steering Group creates a sustainable funding model, without pay-to-play relationship

8. Sensitivity to requirements for international collaboration

9. Minimize adverse legal impacts caused by government involvement (e.g. FACA)

10. Don't break anything that's working today

# ***Part II: Responses to Governance NOI Questions***

## INTRODUCTION TO PART II

The Governance NOI provides that it specifically:

> . . .seeks comment on the structures and processes for Identity Ecosystem governance. This Notice does not solicit comments or advice on the policies that will be chosen by the Steering Group or specific issues such as accreditation or trust mark schemes, which will be considered by the Steering Group at a later date.

This response provides an overview of governance and process associated with formation and operation of the Steering Group. The focus here is various external elements that should inform that internal governance structure of the Steering Group. This response does not seek to address policy issues.

It is suggested, however, that some of the internal governance structuring decisions might benefit from being developed as a part of the effort to derive the stakeholders' substantive problem set during the "agenda setting" and "problem identification" stages of rulemaking (described in section 1, diagram 2). In other words, the types of issues that the Steering Group will be asked to address will affect how it is best governed and structured.

The Participation Governance Model, which informs the structure of this Governance NOI response, reflects an effort to "unpack" the Identity Ecosystem and the processes that support it. It is those processes, such as (i) rulemaking processes to construct private sector Trust Frameworks, (ii) separate rulemaking processes to identify and formalize the larger Identity Ecosystem Framework, and even (iii) rulemaking processes to define the governance structure of the Steering Group itself (the current subject), that the Steering Group (or in the case of (iii), its predecessor initiatives) should be structured to govern. The importance of the relationship of stakeholder needs to Steering Group governance is one reason why these OIX responses are cast in the context of the Participation Governance Model.

Toward that end, it is suggested below that the steering Group be developed through a separate, abbreviated version of the standard five (5) step rulemaking process, engaged in by a broad group of stakeholders (such as those which participated in the NSTIC workshops and other similar organizations involved in standards development and Trust Framework development in the area), who can work together to narrow the issues in the "Agenda setting" step, further refine and develop the issues in the "problem identification," step and finally work together to reach the "decision" step to craft a governance structure the implementation of which best matches the substantive issues with which the structure will be asked to deal.

In response to the asserted goal to “stand up” the Steering Group by the end of 2011, a “straw man” draft Steering Group charter has been prepared and is submitted with this Governance NOI response in an effort to accelerate the movement through the first three stages of rulemaking for the Steering Group structure

# INDEX OF QUESTIONS

This Part 2 of the OIX response has 4 sections reflecting the Governance NOI sections in the order that they occur in the Governance NOI. Also, sub-section references correspond to question numbering in the Governance NOI.

In situations where a series of questions are asked under one NOI sub-section number, specific question numbers have been assigned (and provided in parentheses in the Table of Contents below).

1. Structure of the Steering Group

Questions:

(1.1.1) Given the Guiding Principles outlined in the Strategy, what should be the structure of the Steering Group? (1.1.2) What structures can support the technical, policy, legal, and operational aspects of the Identity Ecosystem without stifling innovation?

(1.2.1) Are there broad, multi-sector examples of governance structures that match the scale of the Steering Group? (1.2.2) If so, what makes them successful or unsuccessful? (1.2.3) What challenges do they face?

(1.3.1) Are there functions of the Steering Group listed in this Notice that should not be part of the Steering Group's activities? (1.3.2) Please explain why they are not essential components of Identity Ecosystem Governance.

(1.4.1) Are there functions that the Steering Group must have that are not listed in this notice? (1.4.2) How do your suggested governance structures allow for inclusion of these additional functions?

(1.5) To what extent does the Steering Group need to support different sectors differently?

(1.6.1) How can the Steering Group effectively set its own policies for all Identity Ecosystem participants without risking conflict with rules set in regulated industries? (1.6.2) To what extent can the government mitigate risks associated with this complexity?

(1.7) To what extent can each of the Guiding Principles of the Strategy-interoperability, security, privacy and ease of use—be supported without risking "pull through"[22] regulation from regulated participants in the Identity Ecosystem?

[22] NSTIC solutions will ideally be used across all industries, including both regulated and unregulated industries. "Pull through" refers to the concept that when implementing an NSTIC solution that touches some regulated industries, individuals or firms implementing those solutions would then find that they are subject to the specific regulations for those industries. This could create a confusing policy and legal landscape for a company looking to serve as an identity provider to all sectors.

(1.8) What are the most important characteristics (e.g., standards and technical capabilities, rulemaking authority, representational structure, etc.) of the Steering Group?

(1.9.1) How should the government be involved in the Steering Group at steady state? (1.9.2) What are the advantages and disadvantages of different levels of government involvement?

2. Steering Group Initiation

Questions:

(2.1.1) How does the functioning of the Steering Group relate to the method by which it was initiated? (2.1.2) Does the scope of authority depend on the method? (2.1.3) What examples are there from each of the broad categories above or from other methods? (2.1.4) What are the advantages or disadvantages of different methods?

(2.2) While the Steering Group will ultimately be private sector-led regardless of how it is established, to what extent does government leadership of the group's initial phase increase or decrease the likelihood of the Strategy's success?

(2.3) How can the government be most effective in accelerating the development and ultimate success of the Identity Ecosystem?

(2.4.1) Do certain methods of establishing the Steering Group create greater risks to the Guiding Principles? (2.4.2) What measures can best mitigate those risks? (2.4.3) What role can the government play to help to ensure the Guiding Principles are upheld?

(2.5.1) What types of arrangements would allow for both an initial government role and, if initially led by the government, a transition to private sector leadership in the Steering Group? (2.5.2) If possible, please give examples of such arrangements and their positive and negative attributes.

3. Representation of Stakeholders in the Steering Group

Questions:

(3.1.1) What should the make-up of the Steering Group look like? (3.1.2) What is the best way to engage organizations playing each role in the Identity Ecosystem, including individuals?

(3.2) How should interested entities that do not directly participate in the Identity Ecosystem receive representation in the Steering Group?

(3.3.1) What does balanced representation mean and how can it be achieved? (3.3.2) What steps can be taken guard against disproportionate influence over policy formulation?

(3.4.1) Should there be a fee for representatives in the Steering Group? (3.4.2) Are there appropriate tiered systems for fees that will prevent "pricing out" organizations, including individuals?

(3.5.1) Other than fees, are there other means to maintain a governance body in the long term? (3.5.2) If possible, please give examples of existing structures and their positive and negative attributes.

(3.6) Should all members have the same voting rights on all issues, or should voting rights be adjusted to favor those most impacted by a decision?

(3.7.1) How can appropriately broad representation within the Steering Group be ensured? (3.7.2) To what extent and in what ways must the Federal government, as well as State, local, tribal, territorial, and foreign governments be involved at the outset?

4. International

Questions:

(4.1) How should the structure of the Steering Group address international perspectives, standards, policies, best practices, etc?

(4.2) How should the Steering Group coordinate with other international entities (e.g., standards and policy development organizations, trade organizations, foreign governments)?

(4.3) On what international entities should the Steering Group focus its attention and activities?

(4.4) How should the Steering Group maximize the Identity Ecosystem's interoperability internationally?

(4.5) What is the Federal government's role in promoting international cooperation within the Identity Ecosystem?

## Section 1. Structure of the Steering Group

*Question 1.1.1 Given the Guiding Principles outlined in the Strategy, what should be the structure of the Steering Group?*

**Summary:**

Please see the diagrams and text in Section 1 describing the Participation Governance Model and how it supports the work of the Steering Group.

**Discussion:**

Please see the diagrams and text in Section 1.

The following are additional general notes and recommendations on the proposed structure.

*Structure the Steering Group for specific intended purposes*

Starting with the obvious: The Steering Group should be structured to most effectively accomplish its goals of fostering the establishment of an Identity Ecosystem Framework that is consistent with NSTIC goals.

Unpacking that statement, there are many such goals. All are related, but each has a slightly different character and requirements. Some, such as the "goal" of fostering and achieving effective Steering Group decision making, are associated with generating consensus among stakeholders about how data/identity systems should be structured.

Independent but related goals are associated with the generation of specific documentation output of the Steering Group and its communication to parties outside the Steering Group participants (such as documentation associated with the consensus view of the Steering Group reflected in the Identity Ecosystem Framework documentation).

Still other goals are more "results" oriented, such as creation of a market in which identity solutions are available that conform to the NSTIC Guiding Principles[23] and other goals and objectives set forth in the NSTIC.

The foregoing sampling of related goals, i.e., group consensus, documentation and communication, and external market effects, and other identified goals will all require different processes to be fulfilled, and different stakeholder representative skills and different resources. It is not realistic (or cost effective) to try to "house" all of this process, personnel and activity within a single organization such as the Steering Group.

*An open Steering Group structure*

[23] The NSTIC Guiding Principles are that Identity Solutions will be Privacy –enhancing and voluntary, secure and resilient, interoperable and cost-effective and easy to use. These are discussed in greater detail in Exhibit 2.4.

In order to effectuate these various goals most efficiently, collaboratively, cost effectively and with a minimum of friction, the Steering Group would be well served to adopt and open structure that enables it to *leverage existing initiatives, to access shared resources, to benefit from stakeholder experience and insights*, *and to foster connections among stakeholders*, and groups thereof, at increasingly comprehensive scales to leverage its efforts. This will permit the Steering Group to in effect "outsource" tasks in a form of "institutional crowd sourcing." It will also allow the Steering Group to serve as a "node of aggregation" within the market that can simultaneously foster interoperability and the corresponding "network effects" of broad adoption to networked information systems.

There will naturally be many separate nodes of activity in pursuit of these and related goals within the plenary and the larger community that it serves. The Steering Group, when it is formed, will be a new "node," and one that can serve a relevant and important function of furthering NSTIC goals and principles through private sector initiative. These various nodes should be loosely coupled with facilitation by the governing board (for the Steering Group Plenary) and by the Steering Group (for the larger NSTIC Identity Ecosystem community), and encouraged to proceed to reflect broad stakeholder participation and expressed views on issues. The Participation Governance Model offers an overall structure for this coupling. The Steering Group offers a node around which NSTIC goals and principles can be pursued and supported within that model. OIX provides a common platform of programs and tools to facilitate this.

*Leverage existing initiatives*

In that model, there are multiple levels and perspectives of Stakeholder interests to address, with each additional stakeholder issue adding to the overall system complexity. An open structure will not solve the issues of complexity directly, but it may provide the Steering Group with greater relevance within that overall community/market and a community consensus platform from which it can seek to address system issues.

In an effort to address the issues associated with system complexity, stakeholder representation, and decentralized authority, the Steering Group should be structured to support, encourage, and interact with existing development initiatives in the data/identity markets that are working to create comprehensive hybrid "technical standards," and those that are working on "legal standards" to support the establishment of uniform *legal* duties, standards of care, and rights across sectors in support of existing and future technical standards.

*Architecting legal solutions to governance challenges*

While the notion of technical standard setting is fairly well developed, the concept of "legal standard setting" is a newer concept. It is well known that broad application of common legal/policy duties can have the effect of helping systems to be more interoperable, thereby reducing complexity, since they can render the behavior of different actors in different systems functionally identical. When there is less variation in the behavior of other legal actors, each legal actor's interaction environment is less variable, which reduces complexity (and reduces risk and cost and increases security, predictability, etc.).

For instance, consider a high level principle that states a commonly recognized duty (that was even reflected in the ten commandments) and that is iterated in all legal traditions: "Thou shall not steal" is a statement of a duty, but is sufficiently non-specific so that it can apply across different contexts. It

doesn't specify that a person should not rob a bank, not steal an apple from the grocer, not embezzle funds from an employer, not take a bicycle from a rack, not use cable TV service without paying, or not make unauthorized copies of software, but it applies equally across all those different contexts and domains. When large populations follow the duty, it makes their behavior more reliable, predictable and interoperable.

Similar "high level" duties are needed to inform the Identity Ecosystem Framework, but tailored to meet stakeholder needs in online data/identity systems that are carried over networked information systems.

These legal duties that are documented in the Identity Ecosystem Framework (and in consistent contractual solutions called Trust Frameworks, and in uniform supporting public law when and as needed), can be best designed and developed through an open structure that uses online and social network tools to enable broad collaboration, participation and input, and using market information mechanisms to enable improvement and innovation of those systems at a scale and pace to match the rate of data/identity system growth. This is the goal of the Participation Governance Model and its open structure. This will allow "for more equity, interaction and especially more moments of co-decision,"[24] that will help to address the challenges of governance for complex, decentralized systems. The Steering Group performs a critical role in this model.

*Dealing with the Challenges of Complexity, Representation and Decentralized Control*

Among the more fundamental challenges of governance in the quickly growing data/identity markets are the complexity issue, the stakeholder representation issue, and the decentralized control issue. Each is intended to be addressed by the Participation Governance Model, which in each case informs Steering Group structure. Each is briefly outlined in the following Exhibits to this Governance NOI response.

*Structure to address complexity*
Please see extended discussion at Exhibit 1.1.1 A.

*Structure to address the stakeholder representation*
Please see extended discussion at Exhibit 1.1.1 B.

*Structure to address decentralized control*
Please see extended discussion at Exhibit 1.1.1 C.

[24] "Internet-Mediated Participation Beyond the Nation State," at page 227, by Bart Cammaerts, (Manchester University Press, 2008) lists these and other variables as desirable for systems that seek greater stakeholder inclusiveness.

*Question 1.1.2: What structures can support the technical, policy, legal, and operational aspects of the Identity Ecosystem without stifling innovation?*

**Summary:**

Please see answer to question 1.1.1

**Discussion:**

Please see answer to question 1.1.1.

Please see discussion of technical, policy and legal standards development as "legislative" function and "operational" aspects as "executive" function in Exhibit 1.1.1 C.

The Participation Governance Model seeks to integrate two types of processes and their respective structures that are broadly applied to elicit group preferences. These are markets (grossly defined) and voting. Markets and voting can elicit group views, preferences, needs, and opinions regarding technical, policy, legal and operational elements. They work together to help establish standards.

For example, consider a typical technical standards development organization (SDO) setting. In an SDO, voting is used to move drafts through development processes (vote to get out of working group, vote to get through technical committee, vote for final approval, etc.). That demonstrates how voting helps a group (the SDO) to reach a single decision (a final specification).

When the finalized specification is released to the public, it is then in the market with other potential solutions. The markets are not required to find a single solution, and the specification may succeed or founder based on the needs and preferences of persons outside the SDO. If the standard is broadly adopted, the markets will have spoken positively that the specification meets stakeholder needs. In that case, voting and markets will have worked together to produce the standard that offered the ultimate benefits sought by stakeholders.

In the case of self-regulatory structures (SROs), such as the Steering Group, there is the additional advantage that the standards produced include standard rules for behaviors, and the creators and the subjects of the rules are the same people, i.e., the stakeholders. Thus, in the ideal setting, the SRO/SDO will represent a microcosm of the stakeholders, and rules development will be more comprehensively informed about stakeholder needs. Similarly, released specifications from an SRO/SDO should enjoy more rapid adoption since they were created by the same group on which they are intended to be imposed. The energy associated with the composition of the Steering Group has its origin in the recognition that the authority to create rules for self governance is valuable.

The challenge and the opportunity here is that the SRO/SDO mechanism cannot be housed in any one entity. The scale of the networked information systems that are called the "Internet" is too broad. Instead, what is needed is a "virtual entity" that is spread out over various organizations and the respective internal voting and external market mechanisms with which they are involved. The Governance of the Identity Ecosystem here has various nodes, of which the Steering Group will be just one. It will need to understand the markets, in order to facilitate the collaboration, understand stakeholder needs, and take the votes that are relevant to affect the markets in a way that is consistent

with the NSTIC vision, and so that it can release Identity Ecosystem Framework standards that gain broad and rapid acceptance in the broader markets (both domestic and international).

For a further discussion of how the Participation Governance model seeks to bring together market and voting mechanisms to elicit group preferences dynamically in an open and transparent governance structure that invites participation at various levels, please see response to Question 2.1.1.

*Question 1.2.1: Are there broad, multi-sector examples of governance structures that match the scale of the Steering Group?*

**Summary:**

There are various authorities that have provided helpful treatments of the relevant factors and challenges of multi-sector organizations and multi-stakeholderism. Some of these are referenced in the notes.[25] While none match the scale of the Internet, each provides some helpful insight into potential solutions for challenges raised by multi-stakeholderism.

**Discussion:**

Challenges of governance – scale and multi-stakeholderism:

Many of the anticipated governance challenges facing the Steering Group relate to issues of scale. The Internet is trans-national. Given its global scale, its nearly ubiquitous deployment (achieved through mobile platforms), and its increasing relevance in the social, commercial and political lives of its users, the group of data/identity stakeholders potentially affected by Identity Ecosystem(s) Frameworks begins to approach that of a significant percentage of the human population. At that scale, multi-stakeholderism starts to become "all-stakeholderism" raising the question of what type of representational structure is even possible at that scale.

Within that broad Internet scale, there are multiple other levels at which "governance" structures can help to build data/identity systems and sub-systems (and sub-systems of those sub-systems, etc.) that address stakeholder needs. Different aspects of such systems will be appropriately standardized and governed at different levels.

The question for the Steering Group is on what level it should logically seek to help provide governance structure to the overall "system of systems" that governs the Internet (where control and authority is distributed) to achieve "Identity Ecosystem Framework" goals. Stated otherwise, on what scale can current data/identity systems be considered consistently reliable, predictable, secure, interoperable, easy to use, *and* otherwise operated consistent with the NSTIC vision?

The push for a Steering Group is a push to have some appropriate governance (a form of "self-governance") occur at an appropriately higher scale to enable the benefits of legal standardization across significant populations of stakeholders. After 1648,[26] the highest level political authority is the nation state, so a U.S. strategy (such as NSTIC) represents the most that one country can do unilaterally. To the extent that the national strategy can spawn a successful voluntary, market based, contractual, sustainable private sector-led set of legal standard solutions, it can be iterated and find influence in markets and populations beyond the traditional political boundaries.

[25] See "Internet –mediated Participation Beyond the Nation State," by Bart Cammaerts (Manchester University Press 2008)(Chapter 1 – Theorising multi-stakeholderism); "Non-State Actors as Standard Setters" Anne Peters, et. al (Cambridge Press 2009)(Chapter 4 "Standard setting at the cutting edge: an evidence –based typology for multi-stakeholder initiatives" by Luch Koechline and Richard Calland).

[26] The date of the Peace of Westphalia, which ended the 30 years war and the 80 years war in Europe and is generally associated with the recognition of the with nation state as the primary unit of international governance.

Of course, the Internet is not confined to one nation. Information easily flows across borders, and efforts to limit that flow are resource-intensive and have varying effectiveness. The Steering Group governance should be configured so that it can realize its important role domestically, and so that it can play an additional role internationally to help coordinate standards across the multiple jurisdictions touched by the Internet.

The Participation Governance Model anticipates a role for the Steering Group that is both domestic and international. Please see the narrative accompanying Diagrams 5-8 in Part 1 of this NOI response.

*Question 1.2.2: If so, what makes them successful or unsuccessful? What challenges do they face?*

**Summary:**

Please see response to question 1.2.1 above.

**Discussion:**

The Participation Governance Model set forth in Part 1 reflects an effort to synthesize the lessons of other similar governance and rulemaking efforts in a variety of sectors and regions. That model is intended to apply the elements of more successful rulemaking efforts in a way that is appropriate for this unique setting which will involve multiple initiatives working at multiple levels on an overall structure toward an "identity ecosystem." The model is intended to foster resiliency, transparency, stakeholder access, and opportunities for participation at multiple levels, efficiently at Internet scale.

For a helpful policy sciences analysis of rule making by non-governmental bodies, See "Self Regulation as policy process: The multiple and criss-crossing stages of private rule making" by Tony Porter and Karsten Ronit, from Policy Sciences (2006). The authors survey dozens of articles relating to private rule making and provide an excellent list of references. The generic 5 phase rulemaking construct that emerged from their study also informed the structure of the Participation Governance Model set forth in Part 1 of this NOI response.

For an empirical analysis of the challenges of extraterritorial governance, and an analysis of the World Summit on the Information Society and the Convention on the Future of Europe, See "Internet Mediated Participation Beyond the Nation State" by Bart Cammaerts (Manchester University Press, 2008).

For a variety of articles dealing with structuring challenges of the governance of transnational initiatives and a helpful discussion of multistakeholderism, See "Non-State Actors as Standard Setters by Anne Peters, Lucy Kiechlin, Till Forster and Gretta Fenner Zinkernagel (Cambridge University Press 2009).

*Question 1.3.1: Are there functions of the Steering Group listed in this Notice that should not be part of the Steering Group's activities?*

**Summary:**

The Steering Group functions should be responsive to Stakeholder needs and should leverage existing resources. As those needs are identified through stakeholder analysis and discussions (that can be hosted by OIX programs and tools), the functions of the Steering Group at both the plenary level and the governance board level should be flexibly established and amended as necessary to be most responsive to such identified needs.

**Discussion:**

There is a huge amount of high quality work being done in the data/identity space, particularly in the technical standards area. The Steering Group should help to "steer," but should not reinvent the wheel. The open structure supported by the Participation Governance Model enables the Steering Group to act in coordination with existing efforts and to compliment their work, and to avoid creating a counterpoint to those existing efforts.

The Steering Group should "look before it leaps" when it comes to establishing standards for the Identity Ecosystem Framework. By collecting information about the Trust Framework market (with the assistance of the OIX meta-data listing service), and about Trust Frameworks in development (through the OIX knowledge center wiki), the Steering Group can best identify potential candidates for standardization and inclusion in the Identity Ecosystem framework.

In addition, it should only evaluate the value and configuration of a formal certification and trust mark program once it has identified market-available or market sustainable data and identity "best practices" that are candidates for standardization. When the Steering Group is ready to adopt standards, it can evaluate whether to have a formal certification program and how that program can be most effectively designed. Prior to that time, the Steering Group may find it sufficient to further its goals by making recommendations to independent Trust Frameworks as they are developed, and to rely on that mechanism to drive adoption of common terms and practices consistent with the identity ecosystem.

The Steering Group should not re-develop and re-deploy existing online resources, but should instead use existing programs and tools. OIX has developed programs and tools in anticipation of their use by both governmental and private parties including stakeholders in all roles. The common analytical and market platform will yield greater interoperability among legal duties, whether they arise by statute, regulation, broad standard form agreements, or more specialized contracts crafted to address narrower contexts in a way that is consistent with the "legal stack." By providing ubiquitous access to Rules, Trust Framework development processes and educational materials, it is hoped that "legal standards" can arise to support and extend the effectiveness of the ubiquitous technical standards that currently drive information network interoperability. Even a small achievement of legal uniformity/standardization can support system interoperability by clarifying the duties of system stakeholders, reducing costs and risks and increasing the value and benefits to all stakeholders.

*Question 1.3.2: Please explain why they are not essential components of Identity Ecosystem Governance.*

**Summary:**

Please see response to Question 1.3.1 above.

**Discussion:**

Please see response to Question 1.3.1 above.

*Question 1.4.1: Are there functions that the Steering Group must have that are not listed in this notice?*

**Summary:**

Effective solutions in voluntary systems may need to more comprehensively address stakeholder needs. The Steering Group should be prepared to accept "scope creep" as a possible artifact of the desirability of bringing together related parties and issues into the discussion.

**Discussion:**

Effective Internet scale solutions will comprehensively address multiple stakeholder group needs. The Steering Group should consider issues from all stakeholder vantage points in an effort to bring all the relevant stakeholders "to the table." To address all stakeholder needs, the Steering Committee may need to consider issues not raised in NSTIC or the Governance NOI (such as liability mitigation strategies, relying party best practices, and data subject obligations and duties) needed to assure system integrity, reliability and interoperability.

The Steering Group should review and consider how and whether it can integrate its efforts with that of the I3S (the "Internet and Information Innovation Sector") under the Department of Commerce cybersecurity green paper.

*Question 1.4.2: How do your suggested governance structures allow for inclusion of these additional functions?*

**Summary:**

The Participation Governance Model described in Part I is an effort to describe how the Steering Group can flexibly incorporate a variety of additional issues and functions. Please refer to the narrative accompanying diagrams 5-8 of Section 1.

**Discussion:**

Please see summary above.

*Question 1.5: To what extent does the Steering Group need to support different sectors differently?*

**Summary:**

The flexibility of the Steering Group Plenary and the overall structure of the Participation Governance Model are intended to enable any special support needs.

Such approaches, if applied, should be carefully crafted to make sure that they don't perpetuate unwanted silos and system interoperability barriers, except where those elements serve stakeholder needs consistent with overall Identity Ecosystem Framework goals.

**Discussion:**

The flexibility and access provided by the Steering Group plenary is designed to accommodate different stakeholders from a variety of sectors. To the extent that the Steering Group plenary supports the ongoing "agenda setting" and "problem identification" activity for a variety of stakeholders from multiple sectors, it can flexibly and opportunistically form more formal processes associated with the "decision" stage of rulemaking as needed for a given candidate element of the Identity Ecosystem Framework standard arising from a particular sector or subgroup of stakeholders.

The transition to more formal "decision" and documentation stage can be fostered by the creation of working groups or committees of the plenary, or other suitable collaboration structures needed to solicit stakeholder group representative views, with support and guidance from the governance board.

In addition, the broader Participation Governance Model assures that different groups of stakeholders will have access to support, tools, programs and information they require to participate and contribute to the Identity Ecosystem Framework construction exercise. They can each pursue the participation experience that they desire, supported by OIX online tools and programs.

Current sectoral and jurisdictional divisions should be attenuated if possible. That means that any different treatment of different sectors or groups in Steering Group matters, if any, should be carefully crafted to not perpetuate unwanted divisions. The main goal should be access and the opportunity to participate for all stakeholder groups.

One of the challenges is that in various jurisdictions and sectors different sorts of data has been treated differently. This has created different stakeholder "expectations" and adaptations in different sectors that introduce dependencies and sometimes resistance to change, even to net positive changes in data/identity system design. Any special treatment of a particular sector should be attentive to not unduly perpetuating unwanted divisions, with sensitivity to the challenges of change, even positive change.

Internet scale solutions will need to be interoperable across sectors. During the transition from current silos to shared data systems, different treatment of some sectors may be warranted to ease the transition. Ultimately, however, the goal of system reliability, predictability and interoperability, which is a prerequisite to the enjoyment of stakeholder control, security, privacy and liability limitation, depends on some measure of uniform treatment of stakeholder groups. Support should certainly be different initially in terms of education, transition services, etc., but that will hopefully not translate into different treatment within data/identity systems themselves.

*Question 1.6.1: How can the Steering Group effectively set its own policies for all Identity Ecosystem participants without risking conflict with rules set in regulated industries?*

**Summary:**

The reference to "regulated industries" is assumed to mean those sectors for which explicit data-related laws are applicable. Please see response to question 1.7 for assumptions made in response regarding use of the term "regulated industries."

Existing data laws and regulations in regulated industries can inform system design, particularly at higher levels of assurance (LOA) and with respect to the Level of Protection (LOP) metric that is proposed to "measure" security.[27]

In a mature Identity Ecosystem, currently data "regulated" industries, such as financial, healthcare and other businesses that handle "sensitive" data will be able to "normatively" cross reference the Identity Ecosystem Framework or Trust Frameworks that are consistent with the Ecosystem Framework for compliance, and rely on services and products made available consistent with those Frameworks.

**Discussion:**

Like Trust Frameworks, existing background law (including the more pervasive presence of background law in "regulated" industries), sometimes establishes duties and standards of care that are relevant to how data is handled.

Conformity to these standards of care leads to more reliable systems, and those in which trust grows and costs are ultimately reduced.[28] Where standards are not present (or if present are not conformed to) systems are less reliable, predictable and interoperable.

As commercially viable systems are developed, it seems likely that the commercial product and service "niche" that is represented by regulated industries in the healthcare and financial space, and other spaces where more sensitive data is handled, will seek to take advantage of the cost savings and customer convenience of using more broadly applicable data and identity systems, as long as those systems are viewed as sufficiently reliable to meet with regulatory compliance requirements in the relevant industry.

Conversely, it is expected that as systems are able to demonstrate reliability, predictability and interoperability in delivering satisfactory security, privacy and liability limitation experiences, the audits and assessments of compliance with legislation and regulation that creates special duties of care (in regulated industries) will be able to normatively cross reference the standards

[27] Note that the LOP metric measures "security" while the LOC (level of control) metric measures those data handling duties that are associated various aspects of "privacy."

[28] Even if there are initial costs associated with adaption to new regulations; at least the standardization saves costs over what a non-standardized compliance regime would cost as businesses would be forced to chase "adequate" compliance without guidance.

created under Steering Group auspices as “comparable” and therefore sufficient for one or another standard of care established under current data regulations.

The concept of “comparability” is applied in evaluations under the FICAM TFPAP program. It can also inform how authorities with auspices in regulated industries can evaluate new approaches to protection, and how the rules of regulated industries can be integrated into the analysis of data/identity specific rules.

*Question 1.6.2: To what extent can the government mitigate risks associated with this complexity?*

**Summary:**

The government can identify and recognize those aspects of Identity Ecosystem Framework conformity that are deemed to satisfy compliance requirements with particular duties of care under existing legislation.

The government can entertain changes to legislation and regulation to incorporate new data/identity services that can satisfy compliance requirements.

**Discussion:**

The government can coordinate regulatory and compliance authorities in a manner to enable the identification of "comparability" between existing data/identity handling compliance requirements and proposed Identity Ecosystem standards to enable the use of more broadly interoperable systems in regulated industries.

As Identity Ecosystem Framework standards are deployed, the government can consider whether to legislative and regulatory standards of care can be modified to recognize the situations in which they might normatively cross reference those broader standards, particularly where the Identity Ecosystem Framework standards form the basis for system metrics that enable easier evaluation of comparability.

*Question 1.7: To what extent can each of the Guiding Principles of the Strategy-interoperability, security, privacy and ease of use—be supported without risking "pull through" regulation from regulated participants in the Identity Ecosystem?*

**Summary:**

See Exhibit 2.4, the "NSTIC Guiding Principles "Unpacking" Tool."

**Discussion:**

As with question 1.6, it is assumed that the reference to "regulated" participants in this question is intended to reference those stakeholders that are subject to specific data security-related laws associated with a particular industry.[29]

While so called "regulated" industries in the data/identity space have the most extensive laws that establish specific duties associated with such things as data collection, storage, transfer, disposal and other requirements,[30] they are still sufficiently underdeveloped (typically because of the fact that most were passed when the Internet was at a much less advanced state of maturity), that they could benefit going forward from a (continuous) refinement to reflect the current state of technology and the growing benefits of Trust Framework and Ecosystem Framework legal/policy standardization in the broader data/identity markets. As a result, there is ample room a private sector led effort, including stakeholders from such regulated industries, to define rules and laws that can work across regulated and unregulated areas.

In fact, with respect to market metrics such as LOP ("level of protection")[31], which is chiefly focused on more traditional notions of "data security," there is ample benefit with exploring solutions in regulated industries such as financial, healthcare and the like to identify those rules and policies that offer those systems greater operational "integrity" which may be gainfully considered for application for certain sectors of more broadly deployed data/identity systems.

In other words, not only are "flow-throughs" not a problem, but each regulated area can be viewed as a form of "pilot project" for the creation of a more comprehensive systems now under consideration. They each can inform elements of LOP metrics, particularly at higher levels of protection. To the extent that existing standards of care associated with established data handling duties can be applied from existing data security frameworks into more comprehensive contractual "Trust Frameworks" there will be immediate interoperability benefits.

Another advantage of folding the regulated data sector directly into the Identity Ecosystem Framework standards process and the larger Participation Governance Model is that one legacy of more comprehensive regulation is that it sometimes enjoys more developed definitions. One starting point

[29] Notably there are dozens of federal laws that provide specific duties of care with respect to some form of data or information. These include, for example those statutes listed in footnote 53 to Exhibit 2.4

[30] For a detailed treatment of some of the significant data "actions" under current law, see the OIX Data Actions Survey Tool at www.openidentityexchange.org.

[31] Not to be confused with LOC, "level of control" which relates to "privacy.

for addressing interoperability across industries and sectors, including regulated sectors, is to harmonize selected definitions to eliminate the "definitional anarchy of identity research."[32]

Following the accomplishment of some harmonization of definitions, it could then be possible to create common provisions for at least the more mechanistic elements of systems (including the legal "boiler plate" in data/identity related agreements under Trust Frameworks). From there, standard form contracts and portions of contracts could be configured and presented as Trust Framework components in an open market to help standardize the Trust Framework development process. The Identity Ecosystem Framework standards should employ definitions and other language that is consistent with that used in the market for which it seeks to establish standards to the extent possible.

Also, existing law and practice provides a useful starting point for the analysis, since current systems are configured to conform with those existing rules and practices which represent a form of de facto standardization, so that a "common" starting point for building Trust Frameworks results. This is not to say that all of the current "regulated" data/identity rules and required practices should be mimicked or carried forward without review or modification; they should not. It is merely to note that existing constructs help to establish a starting point for the analysis, even if that analysis results in a conclusion that existing rules should be entirely reconfigured.

OIX has developed and made public several tools that can help parties engaged in this development activity, including a FIPPs analysis tool to help policy makers and Trust Framework developers to compare fair information practice principles, the Knowledge Center Wiki to aid in the development of legal duties, the analysis of risk and the mitigation of potential liabilities, and the Global Glossary Grid to aid interoperability through providing a one-stop shop for over 1700 definitions from 36 sources on online and telecommunications identity.

[32] See p. 204 of the chapter entitled "Quantitative Content Analysis and the Measurement of Collective Identity" by Kimberly Neuendorf and Paul Skalski in "Measuring Identity: A Guide for Social Scientists" edited by Rawi Abdelal, Yoshiko M. Merrera, Alastair Iain Johnston and Rose McDermott (Cambridge University Press 2009). The authors were referring to challenges of identity definitions and theories in the social sciences, but those same challenges plague the analysis applied for policy and legal standardization. The American Bar Association in collaboration with Identity Commons has put together a Global Glossary Grid, which is intended to help parties to address the issues of definitional complexity.

*Question 1.8: What are the most important characteristics (e.g., standards and technical capabilities, rulemaking authority, representational structure, etc.) of the Steering Group?*

**Summary:**

Please see response to Question 3.1.1 for a discussion of Steering Group participant qualities

Please see response to Question 1.1.1 for a discussion of Steering Group overall characteristics.

Please see Additional Notes to Diagram 5 in Part 1 for July 13 Ten Points of Consensus for discussion of Steering Group expectations.

**Discussion:**

Please see summary above.

*Question 1.9.1: How should the government be involved in the Steering Group at steady state?*

**Summary:**

Please see response to Question 2.2

**Discussion:**

The Governance NOI provides that:

> The government's role in implementing the Strategy includes advocating for and protecting individuals; supporting the private sector's development and adoption of the Identity Ecosystem; partnering with the private sector to ensure that the Identity Ecosystem is sufficiently interoperable, secure and privacy enhancing; and being an early adopter of both Identity Ecosystem technologies and policies. In this role, the government must partner with the private sector to convene a wide variety of stakeholders to facilitate consensus, with a goal of ensuring that the Strategy's four Guiding Principles are achieved.

These statements describe an intention to support and promote appropriate government agenda, within the context of the overall NSTIC and Governance NOI affirmation of the need for and benefit of private sector leadership in Identity Ecosystem Framework development.

The concept of "steady state" should be recognized as relating to basic Steering Group governance process stabilization only, since the rulemaking function of the Steering Group will continue to be dynamic and require flexibility. This is because technology and network infrastructure changes will raise new issues that will require new rules to be considered by the Steering Group.

*Question 1.9.2: What are the advantages and disadvantages of different levels of government involvement?*

**Summary:**

Please see response to Question 2.2

**Discussion:**

It can be challenging to "change course" so the Steering Group design and development exercise should not rely too heavily on the government, for fear of involving the government in a process from which it will be difficult to be disentangled.

Having said that, the government anticipates that it will participate in the ways described in the response to Question 1.9.1. In particular, the role of advocating for and protecting individuals would seem appropriately assigned to most every government, each of which has auspices (and varying levels of authority) over various aspects of the existence of all legal persons within their jurisdiction, including those citizens and resident individuals that were born or naturalized in their country, or business or other entities, formed or operating under local law. Whatever the rights or interests of a person in online data and identity, those rights are associated with a legal person, the rights and authority of which are mostly an artifact that emerges from the local law to which they are subjected.

## Section 2. Steering Group Initiation

*Question 2.1.1 How does the functioning of the Steering Group relate to the method by which it was initiated?*

**Summary:**

The Steering Group will be a private sector-led, stakeholder consensus-based, technical and legal standards setting body.

Similar operational processes and parameters, and cultivation of private-sector leadership, should be applied for its initiation as well. The Participation Governance Model, illustrated in Section 1 can help achieve these goals during the initiation phase.

**Discussion:**

Since the Steering Group is intended to be a private sector led, stakeholder-consensus-based standards/rule making body, the method by which it is initiated should also reflect these values and parameters. The Participation Governance Model is intended to foster this approach.

The Participation Governance Model encourages broad stakeholder participation in each of the five stages of rulemaking/Trust Framework development/standards setting. These rulemaking phases also characterize Steering Group initiation. This is because Steering Group governance will be pursuant to sets of rules relating to all of the elements of the Identity Ecosystem Framework.[33] Those governance rules should also be developed by the stakeholders, with the encouragement, support and convening "push" of the U.S. Government. Like other rules, those governance rules will also be developed in five stages.

*A Model for standard setting in open data/identity markets*

The initiation of the Steering Group should be by a form of "guided consensus building" among different stakeholders and different stakeholder groups, just as its later standards-setting operation is intended to be. With all of the disparate elements operating in the Identity Ecosystem at any one time, it is not possible, or desirable, to seek to centralize rulemaking, operation and enforcement. Instead, there will be many different foci of each such function, each meant to address a different context. The Participation Governance model allows for the cultivation of that diversity of view and needs, but with structure and organization around collaborative rulemaking, systems operations under those rules and collective enforcement mechanisms.

The challenge is to identify mechanisms that can bring the different elements of the Ecosystem together, not in a single entity or organizational structure, but in an overall set of integrated, balanced relationships in the Identity Ecosystem that can help to normalize online social communities, economic markets and political governance structures. The Participation Governance Model is intended to loosely

[33] These include Roles/Responsibilities; Risk Models; Accountability Mechanisms; Policies; Processes; Standards.

couple together different groups and initiatives (while preserving their autonomy) through the use of common support systems and market information systems.

*The Model enables group decision making through support of voting and markets*

The Participation Governance Model applies common OIX tools and OIX market information programs to enable the maximum benefits and availability to each stakeholder group of the two main approaches for stakeholder group decision making, i.e., voting and markets.[34]

The Model recognizes and preserves the relative rulemaking "autonomy" of each Trust Framework initiative (see diagram 3), Identity Ecosystem Steering Group (see diagram 5), and standards development organization (see diagram 5) to set up its own internal governance and voting mechanisms. The Model defers to the internal voting autonomy of existing organizations, which allows each such group complete discretion on how they produce their respective outputs, e.g., Trust Frameworks, Ecosystem Frameworks, and Technical Standards respectively. The Model instead seeks to make these outputs more interoperable by offering a common platform (hosted by OIX) for development and for gathering market-relevant information to coax those independent initiatives into integrated systems.

As a new participant in the Identity Ecosystem Framework, the Steering Group will also have the total discretion under the Model to decide how it wants to cultivate group decision making.
The attached draft Steering Group Charter proposes an open Steering Group plenary where decisions are made by consensus processes, with votes taken as needed, and a Steering Group governance board that employs generally the same approach. As stakeholders participating in the initiation process move forward from current governance rules "agenda setting" and "problem identification" stages to "decision" and "implementation," that initial proposal for a charter can be modified to address stakeholder consensus views.

*Market Mechanisms operate outside of organizations, where multiple decisions are desirable*

While group decision making by consensus and voting mechanisms is characteristic of the individual organizations in the ecosystem, decision making in the larger identity ecosystem is better pursued through market mechanisms rather than voting. Markets here are generally defined as places for the exchange of goods and services. The Participation Governance Model applies market mechanisms to help drive group decision-making when the composition of the groups becomes sufficiently broad that voting mechanisms (which are applicable when a single decision is desired) are too narrow to address multiple factors and allow for multiple results.

Markets themselves are built on common rules, tools and processes. These common rules provide a mechanism for stakeholder self-governance, external auditing and monitoring, and identification of interoperability opportunities with other systems. The Participation Governance Model integrates the disparate efforts of various stakeholder groups and their participants by providing external common analytical tools (such as the OIX knowledge center and WIKI), common definitions tools, common survey tools (such as the data action survey tool), and common information programs (such as the OIX meta data listing service).

[34] See, Networks, Crowds and Markets" Id.

All these common OIX tools and programs uniformly support both single organization rulemaking (and the stakeholder *voting* and consensus processes through which standard rules are advanced through development processes), and multiple organization *market* mechanisms. The use of common tools and programs encourages the various "autonomous" initiatives to interact more easily to identify commonalities and provides the common platform and system interoperability "language" that enables the communication needed to pursue that interaction.

*Inter-group communication is a key first step during the initiation phase*

During the Steering Group initiation phase, one of the key challenges will be to find commonality among the myriad "user groups" of networked information systems, so that they can be brought together in a single Steering Group.

One of the key first steps to putting together "systems of systems" such as the Identity Ecosystem, is to establish a common mode of communication between and among the different systems. OIX public tools and programs "host" Trust Framework development and deployment on a common platform that helps to establish those lines of communication (and renders the communication persistent and reference-able), and makes it more likely that rulemaking decisions by separate Trust Framework rulemaking initiatives will more naturally create interoperable structures, resulting in the desirable outcome of a NSTIC-consistent Identity Ecosystem.

*The U.S. should continue to offer support and encouragement to the stakeholder led processes to self-construct the Steering Group*

The report that is ultimately issued by the Department of Commerce/NIST/NPO following receipt of these Governance NOI responses will help to provide a synthesis of views for Steering Group planning. That report will, however, reflect views through the filter of the U.S. government perspective on the issues. While the report can help to perpetuate good momentum toward getting the Steering Group up and running, it should not be too proscriptive. The private sector has already started to formulate positions and approaches to forming and operating the Steering Group so that it does not have to rely too heavily on government leadership and definition.

*Other forms of government support for initiation*

Another way in which the government can encourage participation and momentum for Steering Group initiation without government direct involvement is to start to publicly explore the various types of future potential incentives that the government is uniquely suited to offer for participation in the Identity Ecosystem. By raising the discussion of such incentives at the initiation phase, it may start a process of brainstorming among the private sector that could help to grow interest in the NSTIC and greater awareness of its potential benefits for all networked information system users.

For example, the question of whether tax credits could be provided for expenditures made by companies for development of Trust Frameworks would likely raise interest. As would the interest of Relying Parties in a discussion of whether tax credits might foster growth of investments in software, hardware, networks and service fees paid to connect to NSTIC-friendly systems. See the further discussion of incentives in the response to Question 2.3.

*Question 2.1.2: Does the scope of authority depend on the method?*

**Summary:**

The source of Steering Group "authority" will be the recognized achievement of positive benefits by stakeholders for participation in the Identity Ecosystem contemplated by NSTIC, rather than authority through compulsion. To the extent that the scope and extent of authority is dependent on stakeholder benefits for participation, it is best to understand stakeholder needs and to engage in activities that indicate to stakeholders that their needs will be addressed by the Identity Ecosystem.

In summary, it seems that the broadest scope of authority of the Steering Group will be achieved through broad stakeholder involvement, including at the initiation stage.

**Discussion:**

There are different types of authority. One type of authority is based on compulsion, i.e. governments have the authority to create and enforce compulsory controls and limitations in certain areas. The authority of the Steering Group will not be compulsory. Instead it will have an authority derived from service; the service of helping to address stakeholder needs by convening stakeholders to engage in effective self-regulation and thereby providing efficacy and the opportunity for self-determination to all stakeholders and supporting the balanced advantages of all Stakeholders using networked information systems.

The Steering Group is intended to work to provide stakeholders with the ability to create standard, consensus-based rules to apply to all stakeholders. It is governance of, for, and by the stakeholders. The government should not apply to heavy a guiding hand at initiation, for fear of robbing the process of its private-sector-led momentum, which can carry over into its later Identity Ecosystem rulemaking work. Too heavy a government presence might prevent stakeholders in the private sector from seeing the Steering Group as an organization that represents its interests, reducing its ultimate authority.

Participation in the Identity Ecosystem will be voluntary, so individuals and entities will only join if it is, on balance, relatively advantageous for them to do so. That means that the authority of the Steering Group will not be derived from compulsory sources (as it is with a some exercises of governmental authority) but rather from providing stakeholders with an advantageous online identity alternative, in their multiple roles (and with respect to whether it addresses their social, economic, political, privacy, security or liability limitation or other needs).

If stakeholders are involved in the initiation of the Steering Group, they are more likely to view its output as representative of their views and supportive of their respective interests.

*Question 2.1.3: What examples are there from each of the broad categories above or from other methods?*

**Summary:**

The scale and context of the Identity Ecosystem framework construction effort are unique.

The Smart Grid Interoperability Panel charter documents the organization of a broad, consensus-oriented body formed to address interoperability issues for a broadly networked system, which is a good place to start the discussion.

**Discussion:**

The scale and context of the current efforts to "normalize" and render interoperable data/identity systems that operate over networked information systems is without precedent. As noted elsewhere, it seems clear that broad adoption is critical to achieve the benefits of the "legal network effect" (and thereby to address privacy, security and liability limitation at broad scale). The systems that best address stakeholder needs are likely to enjoy the most rapid adoption. Therefore, the identification of stakeholder needs early in the process is critical to success.

The Smart Grid Interoperability Panel model was chosen as a suggested starting point for the crafting of a NSTIC Steering Group charter because, even though the SGIP dealt with a different networked system (electricity versus information), and a different scale (U.S. electrical grid versus global Internet), and different stakeholder categories, it is a model that appears to be intended to apply a broad consensus-based, participatory approach to develop and integrate group and subgroup goals. It may, therefore, be a good starting point for the Identity Ecosystem Steering Group discussion.

*Question 2.1.4 : What are the advantages or disadvantages of different methods?*

**Summary:**

Please see discussion in answers to Questions above.

**Discussion:**

Please See Discussion in answers to Questions above.

*Question 2.2: While the Steering Group will ultimately be private sector-led regardless of how it is established, to what extent does government leadership of the group's initial phase increase or decrease the likelihood of the Strategy's success?*

**Summary:**

The answer to this question requires a further division of the "group's initial phase" into functional subparts. Attention to the five stages of rulemaking (see narrative accompanying diagram 2 of section 1) helps to discern the phases where government involvement might be helpful, versus where it might be less productive toward the establishment of a privately-led initiative.

For example, it will be helpful for the Government to provide support and convening leadership during the "agenda setting" and "problem identification" stages of Steering Group initiation.

Government leadership might be less effective (and may be in some ways counterproductive) during the "decision" or "implementation" phases of Steering Group initiation, except as requested by the nascent Steering Group as it coheres.

Government involvement in the "evaluation" phase should be coordinated with the private sector evaluation so that it does not develop a separate line of authority that "forks" away from the goals set by the stakeholders for the market. Evaluation or rules and their "enforcement" should be closely coordinated.

**Discussion:**

One critical variable in Steering Group initiation is the role of the U.S. government. It is essential that the parties recognize, plan for and determine how that role should vary depending on the stage of the initiation process. Planning will allow for the Steering Group to get maximum advantage of unique resources and capacities of the government when such involvement is desirable, but permit government involvement to be easily and non-controversially "dialed back" when it is inconsistent with the NSTIC goal of establishing a privately-led Steering Group, and is less desired by the Stakeholders.

For example, it is recognized that there is benefit from U.S. government support and the exercise of convening authority during the early stages of the Steering Group initiation phase. The Governance NOI's "initiation phase" corresponds to the "agenda setting" and perhaps the "problem identification" phases of rule making. Specifically, the U.S. government may play a role as convener during "agenda setting" (as it has done by convening separate NSTIC "governance" and "privacy" workshops) and "problem identification," (as it is doing through the NOI survey and report of the Governance NOI process). Its influence, however, should not be as prominent during "decision" and "initiation" phases of Steering Group governance rules formation and initiation if the Steering Group is to achieve the desired private sector leadership.

The U.S. government may have a role during "evaluation," as this is the appropriate stage to review whether a set of rules (such as Governance rules) is satisfying group goals. A well functioning Steering Group will reflect stakeholder preferences, rather than government imposed policies, but the government may help to monitor and confirm that the stakeholder goals are being achieved. Coordinated government enforcement of private sector-created rules can help to provide substantial cost savings to the private sector, and can be otherwise consistent with stakeholder interests if it is

consistent with stakeholder expectations. Also, the NPO office and the requirements of NSTIC will continue to have a government component, where monitoring and evaluation might naturally be expected.

The U.S. government involvement should be specifically and explicitly defined and limited as part of the initiation planning, to assure that its role is clear. If the private sector perceives that U.S. government influence of the Steering Group will extend beyond support and convening of private sector parties and past the initiation phase and into operations of the Steering Group, it will elicit a more passive, less engaged response from the private sector, which will undermine the ultimate intentions of the program.

*Question 2.3: How can the government be most effective in accelerating the development and ultimate success of the Identity Ecosystem?*

**Summary:**

The government should focus on what it is uniquely set up to do, and leave it to other private sector actors and to the market generally to do what the government does less well.

It should also encourage stakeholders to "unpack" and better analyze current and anticipated needs to better inform Identity Ecosystem design and development.

The government should encourage the Steering Group to leverage existing initiatives and available tools and resources (SDOs, OIX, academic initiatives, etc.).

The government should provide seed money for pilots (even small amounts can be very helpful to many initiatives) and for helping to jump start and support stakeholder community organizations and stakeholder educational initiatives.

Finally, the government should start to explore creation of cost-effective incentives for private entity participation in governance (e.g., tax credits for investments by companies in interoperable data/identity technologies and NSTIC-consistent infrastructure).

**Discussion:**

The government should focus on what it is uniquely set up to do, and leave it to other private sector actors and to the market generally to do what the government does less well.

The government is set up to make laws (legislative), carry them out (executive) and enforce them (executive and judicial). Each of these functions can be applied to support the development and success of the Identity Ecosystem in different ways at different phases of its development, but the most effective support will be achieved in close coordination with the private sector initiative.

Thus, for example, legislation might be requested by stakeholders to create safe harbors for certain behaviors that support Identity Ecosystem reliability and interoperability goals. Other forms of legislative activity, however, such as using laws to create duties in an effort to curb certain undesirable behaviors on the Internet, may be of limited use on the global Internet which covers multiple jurisdictions, and may merely drive operations offshore. A more effective strategy for both the government and the private sector will be to create a hybrid structure that integrates and coordinates the public law and regulation rules (and the corresponding duties that they create) with those arising under standardized private agreements.

Page 4 of the NOI provides that:

> The government's role in implementing the Strategy includes advocating for and protecting individuals; supporting the private sector's development and adoption of the Identity Ecosystem partnering with the private sector to ensure that the Identity Ecosystem is sufficiently interoperable, secure and privacy enhancing; and being an early adopter of both Identity Ecosystem technologies and policies. In this role, the government must partner with the private sector and to convene a wide variety of stakeholders to facilitate consensus, with a goal of ensuring that the Strategy's four guiding Principles are achieved.

Implementation of the Participation Governance Model presented in this Governance NOI response can help the government to achieve its goals consistent with NSTIC and can help define the appropriate role of the government vis a vis the private sector during the Steering Group design, development, initiation, deployment and operations stages. OIX tools provide information that can benefit all stakeholders (including the government as stakeholder. OIX programs foster communications across the market during both Trust Framework development and with respect to fully deployed Trust Frameworks.

*Leverage existing initiatives and available tools and resources (SDOs, OIX, academia)*

The government has a unique position as a convener. It has already demonstrated that capacity in the calling of the NSTIC workshops and in the positive energy that it has generated around the Governance NOI. Under the stakeholder self-regulatory Participation Governance Model, the source of innovation, solutions and Identity Ecosystem Framework components and participants is the pool of networked information system stakeholders. That stakeholder community has, even in this early period of Identity Ecosystem evolution, generated many groups that have been actively pursuing a variety of technical standard setting and stakeholder community development efforts. These efforts should be encouraged and supported, since they are the engine for the Identity Ecosystem.

The existing efforts should also be seen as a source of valuable information for the future Steering Group work. Integrated systems of information, collaboration and community building will help to encourage the flow of information among the initiatives and with the Steering Group to the benefit of a healthier and faster-assembling Identity Ecosystem.

The government can also provide seed money for pilots (small amounts can be helpful) and for helping to jump start and support stakeholder community organizations.

Since the Identity Ecosystem often uses existing hardware, software, networks and other technology elements, it is possible to test structures, protocols and new systems for a relatively modest cost. As the Steering Group starts to explore potential market "best practices" candidates to be included in the set of Identity Ecosystem Framework standards, it should aggressively fund multiple pilots, and provide other resources to support the proliferation of multiple approaches that can then populate the market. As in nature, a diverse ecosystem will be more sustainable and less subject to the equivalent of population crash as conditions change.

The government can start to explore the creation of incentives for private entity participation in governance and legal standards setting (e.g., tax credits for investments by companies in interoperable data/identity technologies, safe harbor approaches, support for risk spreading mechanisms, etc.).

As mentioned above, the federal government, through its legislative and regulatory authority, has the ability to craft incentives for various behaviors. Those incentives take many forms and can include tax incentives, export incentives, and tax exemptions to entities that help extend identity ecosystem benefits to under-served populations or populations with special identity needs (such as children, incapacitated individuals, etc.), government educational programs and other resources to educate individual and commercial users in a way that creates market demand for certain system features that are consistent with the NSTIC Identity Ecosystem. Starting a dialog about possible incentives can attract attention, support and excitement for the NSTIC programs.

*Question 2.4.1: Do certain methods of establishing the Steering Group create greater risks to the Guiding Principles?*

**Summary:**

Each guiding principle is independent and affects different stakeholders differently. In order to evaluate the potential effects of Steering Group initiation on the Guiding Principles, it is necessary to consider them individually.

Exhibit 2.4.1 of this Governance NOI response presents a Guiding Principles Correlation tool to address particular effects.

**Discussion:**

Please see Exhibit 2.4.1.

*Question 2.4.2: What measures can best mitigate those risks?*

**Summary:**

Please see Exhibit 2.4.1.

**Discussion:**

Please see Exhibit 2.4.1.

*Question 2.4.3: What role can the government play to help to ensure the Guiding Principles are upheld?*

**Summary:**

Please see Exhibit 2.4.1.

**Discussion:**

Please see Exhibit 2.4.1.

*Question 2.5.1: What types of arrangements would allow for both an initial government role and, if initially led by the government, a transition to private sector leadership in the Steering Group?*

**Summary:**

Please see response to Question 2.2

**Discussion:**

Please see response to Question 2.2.

*Question 2.5.2: If possible, please give examples of such arrangements and their positive and negative attributes.*

**Summary:**

Please see response to Question 2.2

**Discussion:**

Please see response to Question 2.2

## Section 3. Representation of Stakeholders in the Steering Group

*Question 3.1.1: What should the make-up of the Steering Group look like?*

**Summary:**

The Steering Group should have a two-part structure with an open plenary, the work of which is facilitated by a governing board tasked with limited administrative and facilitation functions. The plenary would retain substantial Identity Ecosystem development leadership and authority within the two-part Steering Group structure.

The Steering Group plenary should be composed of representatives of different groups of stakeholders that have either a direct or indirect interest in the Identity Ecosystem as conceived by NSTIC, and the stakeholder categories within the Plenary should be subject to modification as data/identity markets change.

Strong consideration should be given to combining the work of the "Internet and Information Innovation Sector" (the "I3S")[35] with the work of the Steering Group. This will affect the composition of the Steering Group positively, by including some stakeholders that might not otherwise participate and by appropriately expanding the discussion to include the three related sets of issues that are covered by proposed LOA, LOP and LOC market metrics.

In addition to the question of stakeholder group representation, there is also the issue of expertise and skill set. The experience, expertise and background of the individual Steering Group Participants should be matched to the intended output of the group. This is where the benefits of the plenary will be most dramatic. A broad plenary organization that is structured for collaboration and the propagation of ideas across the market will provide the benefit of access to a broad range of thinking and skills that can best inform broadly adoptable Identity Ecosystem standards

**Discussion:**

*The Steering Group Two Part Structure*

OIX suggests that question 3.1.1 be rephrased to "how should an open participatory, consensus building legal/policy standard setting organization be organized to continuously maximize participation and access?" The suggested change in perspective is reflected in the suggestion that the Smart Grid model for participation be adopted as a starting point for discussion. In that model, the plenary group is entirely open to all interested parties. Also in that model, the Governing Board (elected from the Plenary) is merely an administrative and operational body that facilitates the accomplishment of the goals of the plenary. In the Participation Governance Model, the plenary is the *head* and the *heart* of the Steering Group, while the Governance Board is just the *hand*.

[35] See Department of Commerce Green Paper entitled "Cybersecutiry, Innovation and the Internet Economy" released by the Department of Commerce Internet Policy Task Force.

The answer to the question is therefore a bit closer to the ideal where the Steering Group "looks" like the Stakeholder group. The Participation Governance model is intended to make the overall governance and participation structure "dynamically isomorphic" with the stakeholder group, even as the stakeholders group itself evolves. An open Steering Group model can take maximum advantage of the Participation Governance Model.

The open plenary structure that was applied in the Smart Grid model and is carried forward to the discussion draft Steering Group Charter (attached), renders the question of Steering Group makeup less "controversial." That is because the plenary is a place where anyone with interest can participate. The emphasis on the plenary will allow a continued focus on broad stakeholder participation and innovation to address needs, not the distraction and inefficiency of attention to strategies to address a scarcity of "seats at the table."

The organization of the plenary into functional groups (as was done in the smart grid setting), for purposes of electing representatives to the Governing Board can also be less contentious by assigning the Governing Board with merely ministerial and administrative responsibility, while leaving more of the "legislative" (aka "Identity Ecosystem Framework crafting") functions in the plenary.

Thus, the smart grid charter model with its two part structure of a plenary and a governing board would seem to fit the needs of the data/identity stakeholder community here, given its diversity, scale and dynamic state of change.

What is the "ideal" relationship of the plenary to the governance board? That is a multifaceted analysis. Some of the relevant variables are discussed in this Governance NOI response. Most of them will be most appropriately worked out among the stakeholders, just as those stakeholders will be relied upon to compose the Identity Ecosystem standards for their self-governance in the data/identity markets. The Participation Governance Model provides a structure in which the necessary discussions and collaboration can naturally take place.

*The benefits of broad representation*

This goal of open participation is also the intention of the Participation Governance Model.[36] The model anticipates alternative avenues to participation, even beyond that of the Steering Group's plenary body,[37] to encourage broad stakeholder participation and to provide alternative mechanisms for participation to suit different stakeholder needs, capacities, resources, and timeframes.

The provision of alternative avenues to participation can help to reduce the pressure on the composition or work of any one path to participation, such as the Steering Group, since there are multiple, alternative pathways to stakeholder participation. As discussed elsewhere in this Governance NOI response, broad and appropriately supported and curated stakeholder participation at the design and development stage will yield system structures (including Trust Frameworks) that are most aligned with stakeholder needs. With broad stakeholder representation, the development work associated with

[36] For an empirical analysis of multi-stakeholderism and its challenges see "Standard setting at the cutting edge: an evidence-based typology for multi stakeholder initiatives," by Luch Koechlin and Richard Calland in "Non-State Actors as Standard Setters" Ibid.

[37] See Diagram 5, Section 1.

Identity Ecosystem Frameworks and Trust Frameworks can be thought of as an elaborate form of "market research." That research will enable systems to best address current and changing future stakeholder needs, which will in turn assure the most rapid rate of adoption of future systems.

*Combine NSTIC and Commerce Department Cybersecurity initiatives*

Strong consideration should be given to combining the work of the "Internet and Information Innovation Sector" (the "I3S")[38] with the work of the Steering Committee, or at least creating robust interaction between the groups. In fact, the substance of the work called for in the Department of Commerce Green Paper entitled "Cybersecurity, Innovation and the Internet Economy" is related to the "level of protection" (LOP) data/identity system metric that is described in Part 1 of this response (see narrative accompanying diagram 3 regarding "LOA," "LOC," and "LOP").

Very generally speaking, the NSTIC relates to assurance and privacy concerns that are primarily associated with the LOA (level of assurance) and LOC (level of control) metrics. The Cybersecurity Green Paper relates to the security and "protection" of data that are anticipated to inform the quantification signaled through the LOP (level of protection) metric. As noted elsewhere, sustainable solutions in the networked information system space will need to be more (versus less) comprehensive. Combining these related efforts will not only save costs, time and resources, but will make accomplishment of their respective goals more likely.

*Steering Group Experience and Expertise*

The representatives on the Steering Group should have the experience, expertise, commitment, and access to resources that will be relevant to the various anticipated outputs of the Steering Group. This is similar to the test applied for participation in many open technical standard setting organizations, which often call for participants to have similar qualities. The Steering Group composition is not just about "agenda," it is also about skill set.

Thus, for example, to the extent that the Steering Group will deal with technology issues, a good portion of the Steering Group should have technical backgrounds. If the Steering group will deal with policy and legal issues, its output may be more readily integrated with existing structures if the Steering Group includes representatives who are familiar with the analytical frameworks, language and approach of legal and policy areas. There is little benefit in asking engineers to write contracts, just as there is little benefit in asking lawyers to write technical specifications. The Identity Ecosystem Framework, like the Trust Frameworks that it is intended to inform, is a hybrid technical and legal document. The Steering Group should include individuals who speak the language of different elements that will go into the composition of these documents, and who are familiar with the concepts, challenges and solution pathways available in their respective areas.

Broad stakeholder representation is not only important to hear and respond to stakeholder needs, it is also important to gain the benefit of the expertise and experience of the many different stakeholders with interest in the area. The Participation Governance Model is not intended to merely to "placate"

[38] See Department of Commerce Green Paper entitled "Cybersecutiry, Innovation and the Internet Economy" released by the Department of Commerce Internet Policy Task Force.

groups by simply letting them be heard, it is built to encourage active participation and the expression of needs.[39]

In fact, the collective skills and expertise of the Plenary will be truly impressive, particularly when it is combined with the public and other Steering Groups through the use of common OIX tools and programs. Those who have witnessed the facility of "crowd sourcing" to solve complex problems have come to realize that there is nothing smarter than groups working effectively together. With appropriate structures in place to facilitate, guide and curate discussion and information flow, this form of "structured crowd sourcing" may be an effective way to help design the legal standards that will guide how these systems work.

OIX programs are intended to provide stakeholders with a chance to both express needs *and* to participate in developing solutions. The multiple voices are brought together through the use of common tools and programs such as those illustrated in Diagram 3 of Part 1 of this Governance NOI response.

[39] See the "Ladder of citizen participation" in "Internet-Mediated Participation beyond the Nation State" Id. at p. 29.

*Question 3.1.2: What is the best way to engage organizations playing each role in the Identity Ecosystem, including individuals?*

**Summary:**

Present clear description of benefits.

Provide multiple pathways and modes of engagement.

Revisit engagement strategies periodically to address changes in stakeholder needs and desires.

**Discussion:**

*Present clear description of benefits*

A clear presentation of the benefits of stakeholder self-regulation will help stakeholders to recognize the advantages of participation and encourage their engagement. This will take patience and creativity as data and identity markets quickly evolve and mature. At present, even the groups that are currently most engaged would be hard pressed to comprehensively describe their needs in the data/identity markets. OIX tools and programs are intended to help stakeholders to analyze potential benefits, and to work with other stakeholder groups to develop comprehensive, sustainable solutions to their respective needs; an integrated structure of stakeholder benefits called the "Identity Ecosystem.".

Participants will see the benefits differently depending on the role that they play in a particular transaction. In the most basic trust triangle, the data subject, the relying party and the identity provider each have their respective needs (including privacy, assurance and liability limitation respectively; with all three also seeking security, reliability and interoperability). Each of those benefits sets will require a different set of duties to be performed by the others. Engagement of all parties will be enhanced if the benefits of scale, mutual promises as contract consideration, and integrated interdependent duties are clearly described.

*Provide multiple pathways and modes of engagement*

Providing multiple different pathways to participation will help to encourage different groups, with different needs, capacities and resources, to participate in different ways. Different people and institutions have different goals and modes of engaging in any structured activity. Providing multiple, different opportunities for engagement in Steering Group Plenary activities, and in the larger Participation Governance Model to accommodate these differences will help broaden participation.

For example, the involvement of individuals and entities may differ. Entities (whether commercial or governmental) are more likely to get involved in Trust Framework and Ecosystem Framework development than are individuals since they are more likely to be involved in handling data about third parties and relying on such systems in normal operations (although the distinction between institutional and individual third party data handling may be diminishing with the expanded use of social networking).

Individuals may be invited to participate in rulemaking efforts (in the manner in which each such Trust Framework or Identity Ecosystem Framework development effort permits), but most individuals (acting

in their own capacity, rather than a representative capacity) are unlikely to have the time, resources or predisposition to participate directly on their own behalf. For these individuals, it will be important to have representation on the Steering Group to advance their interests during development.

Of course, most individuals will be much more likely to be involved as data/identity service users (either data subjects or relying parties), than service providers in the markets through which data/identity services are provided. In the Participation Governance Model, the markets are an important mechanism for stakeholder groups, and especially "user groups," to express preferences (the other being the "voting" within individual Trust Framework initiatives and Steering Groups, etc.). Therefore, cultivation of market information resources for use by the Steering Group will provide it with the benefit of individual participation, even where individual stakeholders cannot directly participate. The OIX Meta Data listing service directly supports this connection.

In addition to relying on the markets, individuals and groups can also express their interests through the publicly available OIX online programs and tools. There, they can find educational materials to help them with decisions about how to best engage in the Identity Ecosystem, and can provide comments on deployed and proposed online identity and data offerings in an effort to affect future development.

*Revisit engagement strategies periodically to address changes in stakeholder needs and desires*

The strategies to encourage engagement will also likely change over time. Initially the effort will need to present a current value proposition to currently cohesive groups. Those groups will have already aggregated around common agenda that reflect existing roles and established commercial propositions and traditional social agenda. One of the challenges will be to identify and describe how new benefits of new data/identity systems address existing needs. It will not always be a perfect fit. Engagement of existing groups will be enhanced to the extent that the Steering Group efforts are shown to be relevant to current needs (and currently perceived future needs).

The opposite is also true; there will also be challenges to engaging newly defined groups of stakeholders. As new groups cohere around new common networked information system goals and online needs, there will also be a struggle to configure systems to address the needs of stakeholders in such new and unfamiliar groupings. The Steering Group will need to anticipate and seek to address the emerging needs of new groups of stakeholders as they arise in the community of stakeholders.

Within the Steering Group Plenary, stakeholder groups should be permitted the opportunity to form at different rates, varying with resources, attention, etc. Notably, the categorization of Plenary members into groups is chiefly important to elect the representatives to the governing board. To the extent that the Plenary retains significant authority and opportunity to engage in rulemaking/framework building, and a structure that is open to new and modified group perspectives, it will not be too late to participate, if a now-nascent group later comes to the table.

In fact, the open plenary structure should be designed to be extendible with new groups being added as the market matures, and groups able to divide and combine to reflect changes in Stakeholder needs. By keeping a focus on addressing stakeholder system needs as the central goal, the evolution of the categories of Steering Group stakeholders can be best accommodated.

*Question 3.2: How should interested entities that do not directly participate in the Identity Ecosystem receive representation in the Steering Group?*

**Summary:**

The Steering Group should have an open structure that encourages participation.

Steering Group participants should be encouraged to be "neutral" in their deliberations, and to look at the big picture issues.

The Steering Group can help direct non-participants to "indirectly" participate through use of the same OIX online tools and programs that are available for use by the Steering Group.

The Steering Group should recognize that most individuals and entities will participate through their "market" activity, i.e., their decisions on which data/identity products and services to use, and so should consult with market information in its deliberations as a "market surrogate" for direct participation in the Steering Group by all (millions/billions) of the potential users.

**Discussion:**

The Steering Group should have an open structure that encourages participation. The Steering Group plenary should employ an open, community-oriented design that is open so that all "interested" parties will have chance to participate in the plenary. An open, accessible, transparent structure will help to assure that every stakeholder that desires to participate is provided with the opportunity to do so.

Steering Group participants should be encouraged to be "neutral" in their deliberations, and to look at the big picture issues. Steering Group participants should be encouraged to "check their hats at the door," and decision-making processes should be designed to discourage behavior that is overly driven by individual agenda, to emphasize collaboration, consultation and compromise to reach common goals. This will diminish the negative impact on stakeholders that are not directly represented in Steering Group deliberations.

Toward this end, Steering Group participants should be reminded that these are voluntary systems. They will not be broadly adopted, particularly internationally, unless they offer desirable "network effects" that include privacy enhancement, security improvement, liability mitigation and other benefits to all parties. If they are not broadly adopted, they will provide lesser benefits. If the full benefits of legal/policy standards for the Identity Ecosystem are to be realized, it will likely be at a scale that will provide incentive to a broader range of stakeholders to participate.

The Steering Group can direct non-participants to "indirectly" participate through OIX online tools and programs. The Participation Governance Model, supported by OIX tools and programs, provides multiple pathways to participation so that even those stakeholders who do not directly participate in the Steering Group or its outreach programs will have multiple avenues available to them to affect decisions.

The Steering Group should recognize that most individuals and entities will participate through their "market" activity, i.e., their decisions on which data/identity products and services to use, and so should consult with market information in its deliberations. In fact, the vast majority of individuals and entities that will ultimately benefit from the work of the Steering Group will never know that it even existed.

This is because those people will participate in data/identity markets, not in meetings, voting and standards-setting deliberations, as a way of expressing their preferences.

The participation governance model integrates the two methods, i.e., voting and markets, of group preference identification and expression. Because the Steering Group will establish standards for the Identity Ecosystem and the identity ecosystem will affect social communities, commercial markets and political governance structures, interested entities will have ample opportunity to express their preferences through various mechanisms in each arena.

*Question 3.3.1: What does balanced representation mean and how can it be achieved?*

**Summary:**

The term "balance" suggests stability due to even weighting, or an equipoise between contrasting, opposing or interacting elements. "Balanced representation" would tend to indicate these qualities applied in metaphorical terms with regard to the functioning of the Steering Board.

To achieve "balanced representation" the Steering Board might consider:

First, trying to solicit views from already-identified stakeholder groups on other potentially relevant stakeholder categories, and inviting participation by the identified groups.

Second, recognizing that "dynamic balance" will be needed over time, so that the Steering Board should be structured to anticipate and invite change in the composition of that board as time goes on and markets and online communities change.

Third, recognizing that balance will always be a challenge and subject to critique of one group or another, but that the negative effects of any inadvertent imbalance can be mitigated by assuring multiple pathways to participation.

Fourth, recognizing that balanced representation is not just about counting heads, it is also about providing participants with balanced and relevant information to help them to make balanced decisions, and pointing out to them the benefits of more inclusive composition of the Steering Board and a more "balanced" set of standards that grows the group of potential adopters, increasing the benefits to all participants.

**Discussion:**

First, try to solicit views from already identified stakeholder groups on other potentially relevant stakeholder categories.

Existing, self-identified stakeholders each maintain relationships with various parties. Those existing stakeholders (such as the parties represented at the Governance NOI workshops), know the identities and roles of the parties with which they themselves interact. Soliciting the views of identified stakeholders on the pool of potential additional stakeholder groups that might warrant representation in the Steering Group Plenary will at least identify the penumbra of possible groups that might be interested, and that should appropriately be involved in the future.

Question 3.3.1 points out a fundamental challenge of "multi-stakeholderism," which has been the subject of a number of studies.[40] That is the struggle to achieve nominal and functional "balance," in a representative body, primarily due to an inference (probably accurate) that deficient representation will be a disadvantage and that "excess" representation provides an unfair advantage with respect to the work and outcome of the work of the representative body.

[40] See authorities listed in note 4 above.

There are multiple potential points of "balance." Finding those points will be a challenge since any small group in the data/identity space will be asked to try to represent and consider the interests of dozens of groups and roles, reflecting thousands of commercial, social and governmental entities and hundreds of millions of individual people (in a U.S.-based Identity Ecosystem). Clearly something is likely to get lost in the representation "translation," making "balance" a soft and moving target.

A hint at some of the representation requirements is offered by considering that since the Steering Group will be engaged in rulemaking for standard form agreements, it will benefit from the inclusion of all identifiable stakeholders groups required to construct comprehensive solutions. This is because adoption of voluntary systems is enhanced if "market research" is done in the first instance, i.e., including stakeholders in the design process. The Steering Group is just one way for people to participate.

Notably, the Plenary portion of the Steering Group is open ended, mooting the "balanced representation" issue at that level. At the governing board level, the issue is muted by the limitation of governing board authority. Notwithstanding that limitation, the governing board will have some ability to centralize the decision making of the Steering Group (even if it is by the decisions as to allocations of development resources and the like). As a result, there will still be interest in the mechanisms that can be applied to assure that the governing board also demonstrates the benefits of "balanced representation."

This is where the benefit of the Participation Governance Model can be realized. Under that model, there are multiple pathways to stakeholder participation, taking the burden off the Steering Group "balance" as a market critical variable.

For practical purposes, the Steering Group governance board is probably limited to no more than a few dozen individuals, at most. As is the case with drawing maps or creating models, the smaller the numerator of representation in relationship with the denominator of stakeholders, the more "detail" tends to be lost or obscured. As noted above, something is bound to be "lost in the translation." That is intrinsic to the exercise of representation.

That suggests a value in not "putting all your [participation] eggs in one [Steering Group] basket." In other words, do your best to get "balanced representation," on any particular group, initiative or board (such as the Steering Group), but also rely on the diversity of stakeholder participation opportunities under the Participation Governance Model to reduce the pressure on any one group to "get it right." Also, don't worry if the "balance" requires periodic adjustment. In fact, such change should be planned for.

Second, recognize that "dynamic balance" will be needed, so expect and invite change in the composition of the Steering Board as time goes on and markets change.

As noted elsewhere in this Governance NOI response, Stakeholder needs are changing rapidly as the data/identity markets and communities mature. As the markets and communities mature, stakeholder needs change, and new stakeholder groups arise. The Steering Group will maintain maximum relevance to the extent that is it able to evolve to meet the evolving needs of stakeholders.

Third, recognize that balance will always be a challenge, but the negative effects of imbalance can be mitigated by assuring multiple pathways to participation.

Fourth, recognize that balanced representation is not just about counting heads, it is also about providing participants with balanced and relevant information to help them to make balanced decisions, and pointing out the benefits of more inclusive composition of the Steering Board.

Ultimately, the Participation Governance Model positions the Steering Group to interact directly with the data/identity market through shared development tools and market information mechanisms. The access to broader domestic and international markets is an important element of how balanced representation can be achieved. In effect, by turning all of the market participants into Steering Group participants, through observing and analyzing their choices in social and commercial settings, and by providing them with the ability to express preferences more explicitly in online comment and feedback mechanisms, the Participation Governance Model incorporates market information mechanisms directly into rule making processes.

*How the benefits of comprehensive solutions will affect stakeholder participation*

All stakeholder groups benefit if a greater diversity of stakeholders is represented at the Steering Group level. That is because more comprehensive solutions are more scalable more cheaply (see below discussion). Therefore it is in the interest of groups already involved to seek to attract and recruit additional participation so that more parties are "inside the tent" so that the stakeholders that adopt the voluntary Identity Ecosystem Framework will be encouraged to take the steps needed to expand representation on that group

Many successful Trust Framework development projects to date have been of more limited scope than that anticipated for the identity ecosystem and even larger Internet scale systems. They have been confined to operations to enhance a specific type of data/identity benefit. Broadly interoperable systems will not have the advantage of the more finite solutions, but there are some distinct advantages.

*Question 3.3.2: What steps can be taken guard against disproportionate influence over policy formulation?*

**Summary:**

As with Question 3.3.1, provide stakeholders with multiple different pathways to participate and express their views.

The Steering Group should be structured so that the open Plenary, with its working groups and committees, is the primary source of work on Identity Ecosystem Framework standards.

**Discussion:**

The Steering Group plenary should retain the primary Identity Ecosystem Framework creation responsibility, with the scope of work of the smaller governing body carefully tailored to do the things that cannot be done by the Plenary, such as being a facilitation body for the rules development work in the plenary.

If there are groups in the plenary that desire to pursue a particular issue for consideration in the Identity Ecosystem Framework, their efforts should be supported, and their idea made available for consideration in the larger Steering Group plenary and data/identity market community. In fact, it is the combination of those voices brought together which is the stuff of which the Identity Ecosystem Framework will be built. OIX tools and programs are available to support that ongoing multi-group conversation.

*Question 3.4.1: Should there be a fee for representatives in the Steering Group?*

**Summary:**

To the extent that a significant fee for representatives in the plenary could create a barrier to participation, it should be avoided if possible.

It may be possible to raise funds for Steering Group operations through fees generated in the Identity Ecosystem Trustmark program. Fees could also be applied to various system users for various types of Identity Ecosystem use.

There may also be an Identity Ecosystem penalty regime that could generate fees to cover operations.

The nature of the necessary revenue structure is dependent on costs of operating the Steering Group. Until the magnitude or range of those costs is better known, it is difficult to address the structures of potential revenue sources.

**Discussion:**

Please see summary above.

Use fees:

As stakeholder groups' benefits become clearer, the value proposition for such groups will also become clearer, which will also clarify where some of the potential appropriate points of revenue extraction might present themselves.

It is a typical problem of infrastructure, even virtual infrastructure such as the Identity Ecosystem, that participants are reluctant to pay for common infrastructure. Luckily, there need not be a single fee; but a variety of fees for different uses of the Identity Ecosystem in different contexts might be imposed. This would spread out the "user fees" more broadly, reducing their impact on any one individual or group, and allowing each such fee structure to be tailored to the circumstance in which it will be imposed.

The broad application of a fee helps to avoid free rider and secondary free rider problems described in game theory analyses of how groups pay for infrastructure.

*Question 3.4.2: Are there appropriate tiered systems for fees that will prevent "pricing out" organizations, including individuals?*

**Summary:**

If a fee structure were applied, a tiered structure might make sense.

It might be a challenge to identify the basis for the fee gradations. For example, would it be based on scale built on participant revenues, number of employees, number of customers, number of interactions, etc.?

OIX online tools permit all stakeholders to participate with no charge, so that even if groups or individuals were "priced out" by a particular fee structure, they will not be disenfranchised, and could easily find more resource-appropriate ways to participate.

**Discussion:**

Please see summary above.

*Question 3.5.1: Other than fees, are there other means to maintain a governance body in the long term?*

**Summary:**

See response to Question 3.4.1 above regarding some potential revenue generation opportunities.

To save costs, and therefore reduce fees generation requirements, the Steering Group should "outsource" work by piggybacking onto existing standards development organizations and to programs and tools offered by OIX.

**Discussion:**

Fees are only needed to pay costs. Cost reduction mitigates revenue generation pressures. The best way to reduce costs is to not generate them in the first place. That means getting things done for free wherever possible. There are a variety of available resources around that could help the Steering Group to achieve sustainability.

Program structuring should consider areas of significant "outsourcing," such as outsourcing some enforcement functions to government entities (such as the FTC) and to private Trust-Framework-specific enforcement mechanisms. To the extent that enforcement is "outsourced," it will be important to closely coordinate with outside enforcement authorities (particularly governments) to make sure that their enforcement activity is consistent with the standards established by the Steering Group, and not expanded unilaterally by the relevant enforcement authority.

Some elements of the research and development work of the Steering Group could be "outsourced" to any of a variety of current standards development initiatives and other initiatives.

Use OIX tools and programs. In his article "The Financial Crisis and Organizational Capability for Policy Implementation" by Lant Pritchett,[41] the author argues that the ability to engage in policy implementation is at least as or even more important than the policies themselves. Implementations have their own cost profiles. Luckily, both the development of the Identity Ecosystem Framework and its deployment are already within the capabilities of existing OIX tools and programs. This means that the implementation of the development of those policies (the "rulemaking") and the implementation of their deployment (their adoption and iteration in the market) will be supported by OIX. This will enable a greater likelihood of success with policy implementation.

[41] In "New Ideas for Development after the Financial Crisis" Ibid. p.215

*Question 3.5.2: If possible, please give examples of existing structures and their positive and negative attributes.*

**Summary:**

There are several excellent articles in the notes[42] that touch on the various factors, including resource availability and funding.

**Discussion:**

Please see summary above.

[42] See e.g., "Conceptualizing the use of public-private partnerships as a regulatory arrangement in critical information infrastructure protection." By Dan Assaf, in "Non-State Actors as Standard Setters" Id.

*Question 3.6: Should all members have the same voting rights on all issues, or should voting rights be adjusted to favor those most impacted by a decision?*

**Summary:**

Voting structures should be built to support the processes associated with the types of decisions involved.

**Discussion:**

It is extremely tricky to determine voting structures prior to the time that the types of decisions to be voted on are identified. For example, while majority rule works well when there are two alternatives, it creates what are called voting "pathologies" where multiple choices are presented.[43]The question of weighting of votes is premature prior to the determination of what it is that will be voted on, and whether there are alternative mechanisms to identifying and gathering consensus around group preferences. For example, processes may be constructed around consensus building mechanisms.[44]

To the extent that the Steering Group is structured with a focus on retaining in the plenary the energy and the ability to make decisions, voting rights could fruitfully be defined by working groups within the plenary to satisfy needs of that particular context and group. From this perspective, voting rights will vary, but not by a formulaic prearrangement, but rather as another iteration and expression of stakeholder consensus and decision making processes.

Of course, where a particular body or group is constituted and is designed to operate in a particular context, the question will remain on how votes should be structured. First, there will be some matters for which different t percentages of vote will be needed, which has the effect of shifting the power of each vote. This is typical in all corporate bylaws, where in the section dealing with Board and or Member voting usually spells out that some votes must be by super majority, such as the power to dissolve the organization, the power to sell significant assets and the power to amend the bylaws.

[43] See chapter 23 "Voting" in "Networks, Crowds and Markets – Reasoning about a Highly Connected World" by David Easley and Jon Kleinberg (Cambridge, 2010) for a description of the "Condorcet Paradox" and other voting "pathologies." The chapter also explores what types of voting systems can produce group ranking for three or more alternatives. In section 23.7 entitled "Voting as a Form of Information Aggregation" the authors explore the use of voting, not as a way of resolving differences, but of discovering group preferences.

[44] See discussion of the consensus/conflict dichotomy in the chapter entitled "Theorizing multi-stakeholderism." Id. chapter 1 of "Internet Mediated Participation Beyond the Nation State" Ibid.

*Question 3.7.1: How can appropriately broad representation within the Steering Group be ensured?*

**Summary:**

Please see discussion above in response to sections 3.2 and 3.3 relating to the enfranchised plenary section of the Steering Group.

**Discussion:**

Please see discussion above in response to sections 3.2 and 3.3 relating to the enfranchised plenary section of the Steering Group.

*Question 3.7.2: To what extent and in what ways must the Federal government, as well as State, local, tribal, territorial, and foreign governments be involved at the outset?*

**Summary:**

The National Strategy anticipates that the Steering Group will be run by the private sector. This is consistent with the U.S. Federal government's approach in a variety of critical infrastructure coordination issues[45] and represents a heightened awareness of the central role of the private sector in developing data and identity markets at Internet scale.

The commercial sector will design, develop and deploy the systems that will be used by governments to achieve their respective goals. The governments have a role as users of the services, and their views should be presented with other stakeholder groups. Also, government entities operating at all levels should be included in the plenary, not in a special category, but like any other stakeholder group with special needs.

Governments also have a role as auditor/monitor of last resort within a given jurisdiction. They will require information to fulfill this role. Using OIX tools provides a view of the market that can be used by participants and monitors alike.

**Discussion:**

Please see summary above.

[45] Consider the critical infrastructure protection (CIP) program formed for telecommunications, electricity, financial sector, etc. with the participation of private organizations.

## Section 4. International

*Question 4.1 How should the structure of the Steering Group address international perspectives, standards, policies, best practices, etc?*

**Summary:**

Structure the Steering Group for collaboration

Structure for investigation and review

Structure for replication

Structure to gather information from new markets for legal and policy products and services based on Trust Frameworks.

Structure for Steering Group process evolution

Structure for participation

Structure to use available resources and tools

Structure for "quick wins" in interoperability of international legal standards

**Discussion:**

*Structure for collaboration*

The Steering Group will be most effective if it is most "plugged in" to international data/identity markets, allowing for more opportunities for both "inputs" and "outputs" of the Steering Group to be coordinated with other Trust Framework initiatives at Internet scale. Data/identity markets and systems are global, since the "service area" of many of the products and services relied on by stakeholders in those markets and systems is at Internet scale. The Identity Ecosystem Framework as contemplated by NSTIC will be strongly affected by those products and services that arise in the private sector worldwide, even if it is mostly focused on the needs of U.S. domestic stakeholders, and others affected by U.S.-based rules.

The Steering Group could gainfully be structured so that it can cultivate relationships with and among existing international technical, policy and legal standard setting bodies, governments, and international initiatives that touch on markets related to the NSTIC vision of the Identity Ecosystem. Useful collaboration structuring tips may be gleaned from examination and review of the governance and decision making structures of *technical* standard setting bodies that work in the international arena.

In addition, examination of the structures of *policy/rule making* bodies (such as the OECD, World Economic Forum, the World Bank, the International Monetary Fund, and many others can help to identify relevant programs, approaches to group decision making across cultures and borders, and

anticipate challenges and other potential variables to fostering international dialog. Other literature can provide additional examples of organizations that may provide structuring ideas.[46]

Consideration might be given to whether the Steering Group plenary could have a special "international observer" status to promote flow of information, even if the focus is on an Identity Ecosystem originating from the U.S.

*Structure for investigation and review*

In the initial stages, before the Steering Group is ready to elevate selected "market best practices" as candidates for standardization of FIPPs, NSTIC Guiding Principles, and other Stakeholder-based principles, the work of the Steering Group will involve significant efforts to better understand the data/identity market, and the effects of Ecosystem Framework standardization on those markets.

The Steering Group should be structured to enhance the ability to collect information and to disseminate it to Steering Group members, SDOs, Trust Framework initiatives, and others to inform their work. This could mean, for example, that the Steering Group has substantial authority to arrange its information gathering and dissemination programs. OIX programs and tools exist to help fill this need.

*Structure for replication*

It is not just the rules of data handling and identity management that benefit from standardization (in the form of the Identity Ecosystem Framework). There is also a benefit to seeking international standards for the *processes* through which those initial and future standards will be derived at the national or regional level. In other words, there is benefit in standardizing elements of governance and community structures themselves. Standard processes for community and governance interaction can yield greater opportunities for substantive standards and greater interoperability toward international standards as well, while still recognizing, accommodating and supporting local mores as well.

The Participation Governance Model anticipates multiple national and regional Steering Groups in the early periods (See section 1, diagram 3). Participation in that international Steering Group community will offer the U.S. Steering Group substantial additional international collaboration opportunities. To the extent that all such Steering Groups use OIX tools and programs, they will be able to communicate needs, solutions and innovations across jurisdictions more easily.

The Steering Group should be structured to promote adoption of a general "Steering Group" model, based on use of a common organizing charter form, as a basis for common structure for other national and/or regional Steering Groups to foster a "community" of Steering Groups that can collaborate in a more structured fashion based on commonalities of organization and operation fostered by common governance documentation.

[46] See "Non-State Actors as Standard Setters," by Peters, Koechlin, Forster and Zinkernagel (Cambridge Press, 2009)(Interdisciplinary policy sciences research including chapters dealing with multiple regions, contexts and other variables); "New Ideas on Development After the Financial Crisis" edited by Nancy Birdsall and Francis Fukuyama (Johns Hopkins Press, 2011 (Examines new resource and other realities for international development organizations); and "Internet-Mediated Participation Beyond the Nation State" by Bart Cammaerts (Manchester University Press, 2008)(offers empirical analysis of international multi-stakeholderism with focus on the World Summit on the Information Society and the Convention on the Future of Europe).

It is reasonable to wonder whether the anticipation in the Participation Governance Model of the creation of multiple, separate national and regional Steering Groups won't merely perpetuate and harden jurisdictional silos and system rules/policy differences. However Rome wasn't built in a day, and neither will international standards be built instantly for data/identity markets. The separate Steering Group structure will permit appropriate autonomy of multiple Steering Groups representing different jurisdictions, but the use of a common Identity Ecosystem governance, analysis, market and Trust Framework development platform will encourage collaboration and communication among Steering Committees, bridging existing gaps.

The current NSTIC appears to be domestic U.S. focused first, and international second. This is certainly appropriate for a national strategy, but even the first letter of "NSTIC" (which announces it as the "National" strategy) suggests that it is not anticipated that international representatives would be included directly in the effort at its inception. This is perhaps appropriate at this stage of market maturation, and may be necessary given the limitations to U.S. enforcement efforts in the area.[47]

The participation governance model accommodates both the NSTIC U.S. focus, and the clear need for close working relationships internationally. As illustrated in diagram 5 of Section 1, the open, public availability of OIX analytical and data/identity market information tools (in the OIX Knowledge Center and the OIX Meta-Data Listing Service) provides a platform for collaboration among initiatives launched in different jurisdictions or sectors. These tools are commonly available to all initiatives, and all members of the public, whether or not they go though the formal process of forming a Steering Group of other body through which to act collectively.

The intention of the Participation Governance Model is to provide an extensible platform on which each national and sectoral approach can be developed and migrate at its own pace toward standards that are identified in the marketplace as best practices and then standardized and made available for voluntary adoption at Internet scale. All participation is voluntary, so the adoption question for all participants will be whether the "network effect" of participation in a particular Trust Framework or even a particular Identity Ecosystem Framework is sufficiently compelling, given their individual participant needs in varying roles. For many stakeholders and data/identity system uses, international interoperability across borders and cultures will be desirable and valuable and will help drive adoption of standards at Internet scale.

*Structure to gather information from new markets for legal and policy products and services based on Trust Frameworks*

The creation of systems at Internet scale presents a classic international market multi-jurisdiction problem. Since there is no one legal authority that has jurisdiction over the entire system, reliance cannot be placed on any one set of laws, regulations or government enforcement authority for the assignment of uniform duties to make system actors behave reliably and predictably.

[47] For example, the recent Department of Commerce Green Paper entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework suggested that industry will come up with standards (as in the NSTIC model) that could then be enforced by the FTC. FTC jurisdiction is limited internationally. Jurisdictional limitations such as this are the reason that enforcement mechanism for Internet scale systems need to also rely on system-based incentives and penalties and contract-based resolution mechanisms.

Contracts step in where local law leaves off to help bind global systems together. For example, worldwide financial markets are subject to local laws, but are linked by various standardized contractual and other arrangements (all financial instruments rely on specific contract terms). Similarly, data and the users of networked information systems are subject to local laws, but standardized contracts can help to link together systems across jurisdictional boundaries.

Recognizing that international law is mainly contract law, and that drafting contracts is a form of rulemaking, the Steering Group should be structured to interact directly with the parties that are engaging in Trust Framework rule making creation worldwide so that Steering Group efforts can be most closely aligned with what is going on in the relevant markets. In this way, the Steering Group will be able to best discern potential candidates for inclusion as "standards" in the Identity Ecosystem Framework that will be most relevant and useful at Internet scale.

In order to come up with "drafting solutions" in the Identity Ecosystem Framework that account for disparate stakeholder needs, it is useful to create mechanisms for identifying commonalities and establishing consensus among groups of legal entities as to their common needs, and the duties of others that are prerequisites to the fulfillment of those needs. While laws create duties that are typically compulsory within a jurisdiction, contracts are voluntary. Those standard form contracts that best address multiple stakeholder needs in an integrated fashion will likely enjoy the most rapid adoption.

*Structure for Steering Group process evolution*

Given the dynamic nature of data/identity systems carried on networked information systems, the Steering Group should be structured to permit maximum organizational flexibility, both during the initiation phase and following the initiation of "normal" operations. During the initial stages of Steering Group work, the Steering Group Charter should be crafted to anticipate a "phased approach" to Steering Group formation where the initial phase of Steering Group activity is dedicated to investigation, information gathering on existing Identity Ecosystem components and the like. Flexibility as to governance at this stage will keep the organization open to innovation as to how it can most effectively interact with the international stakeholders and authorities

*Structure for participation*

Under the Participation Governance Model, the Steering Group can liaison with other international Steering Groups and with international Trust Framework initiatives at various levels of development. The Steering Group should consider a structure that will enable it to deploy the most effective programs and to pay attention to matching its interactions as appropriate with the five structured stages of Ecosystem Framework development of different initiatives in different countries.

*Structure to use available resources and tools*

The Steering Group should preserve resources and take advantage of existing sources of relevant information by using the open tools and programs of OIX as a common analytical and development platform. To the extent that multiple parties, Steering Groups and Trust Framework initiatives internationally use common development tools, interoperability of legal and policy standards can be enhanced.

*Structure for "quick wins" in interoperability of international legal standards:*

The Steering Group should be structured to gather information about potential opportunities to build both connections and interoperability among systems both in the near and long term.

As an example of how this might work, consider that among the various metrics that might be pursued system wide, (such as LOA, LOP and LOC), LOA may lend itself most readily to standardization, since it deals (at least in part) with objective and statistically testable (and therefore more accessible) questions of demonstrable proof in identification, authentication and authorization practices.

If a decision is made to focus on LOA metrics as a source of early quick wins, this would also inform Steering Group Governance. For instance, since the level of assurance is of value and interest to *relying parties* worldwide, the Steering Group governance structure should include representatives of relying parties in the discussion.

Participation of relying parties in Steering Group processes will also help with the development of the level of protection (LOP) metric, which will be of greatest interest to identity providers and other data handlers. Having the relying parties at the table for the discussion of the LOA metric, from which relying parties benefit, will simultaneously being them for the table for the discussion of the LOP metric, and its reliance on so-called "RP-BP" (relying party best practices).

*Question 4.2: How should the Steering Group coordinate with other international entities (e.g., standards and policy development organizations, trade organizations, foreign governments)?*

**Summary:**

Please see discussion under heading "Structure for Collaboration" in response to question 4.1 above. See Diagram 8 of Section 1.

**Discussion:**

Please see discussion under heading "Structure for Collaboration" in response to question 4.1 above. See Diagram 8 of Section 1.

*Question 4.3: On what international entities should the Steering Group focus its attention and activities?*

**Summary:**

Liaison relationships can maximize those situations where existing Steering Group members are already involved with other "international" groups.

Technical standards groups should be an initial focus.

Policy standards groups should be a separate focus.

International governments and their subdivisions that are seeking new or modified rules in the area (which function as *de facto* standards) are another potential focus.

**Discussion:**

The strength of the Steering Group will be its stakeholders. Many of its stakeholders will have already been active participants in related organizations. The Steering Group should seek to "piggyback" on the existing relationships of Steering Group members to other groups

It may be most efficient to do a survey of Steering Group members, both from the plenary and from the governing board, to identify the organizations with which they are already involved. This information might also be solicited as part of the initial Steering Group assembly process. Then, those who are involved with other organizations could be asked to play the role of liaisons with those organizations, both reporting to the Steering Group on their activities, and reporting about the Steering Group activities as to those other respective organizations. This helps to establish more "lines of communication" from which to build an international Identity Ecosystem community.

Open discussions and relationships with technical standards development groups can help to identify the status of international technical standards that the Trust Framework legal standards will be built to support, and may also provide some models of how the Steering Group might be structured.

Policy standards groups can help inform how the Steering Group can most effectively deal with governance, standards development processes and intellectual property issues in a context where the process "output" and "deliverables" may be closer to Trust Frameworks than that of technical standards groups (where the output is copyrighted specifications and patent cross licenses).

*Question 4.4: How should the Steering Group maximize the Identity Ecosystem's interoperability internationally?*

**Summary:**

The Steering Group will be involved in a legal/policy rules standards setting process to inform private sector contract-based data/identity solutions at Internet scale. By embracing the concept of viewing legal duties established in the enforceable agreements under Trust Frameworks as a new form of data/identity system "specification," the Steering Group can help build data/identity infrastructure at Internet scale.

In terms of output from the Steering Group, "interoperability" is an emergent phenomenon the value of which increases with greater adoption of the Identity Ecosystem Framework. Adoption in open market based systems is dependent on whether the product or service meets stakeholder needs. The enablement of broad participation and input into the Steering Group will make it more likely that the U.S. Identity Ecosystem will gather momentum internationally, and help drive its adoption as a locus of interoperability.

In terms of input to the Steering Group, in the standards context, deliberate adoption of selected portions of existing international standards can yield international interoperability benefit with little effort. If the members of the Steering Group identify one or more elements of an international system that they believe are consistent with NSTIC goals, that section could be "normatively cross referenced."

**Discussion:**

This proposal describes a model that is a new hybrid of traditional technical standards setting approaches and traditional rulemaking (as described in policy sciences literature noted in this Governance NOI response). As described below, this hybrid approach enables governance bodies at various levels across the Internet to simultaneously address standards for both technology tools and legal rules, which when integrated in Trust Frameworks, together form the virtual "plumbing" whence reliable, normalized information network infrastructure can grow.

*How does "rules standardization" resemble "technical standardization?"*

We have a great deal of experience of how to make technology reliable. Technical specifications that capture standards are as old as the notion of interchangeable parts. Technology standards offer multiple benefits to individuals, commercial interests, and society generally. They increase reliability and system resiliency; they lower costs for all standardized system users; increase reliability, predictability, interoperability, safety; and reduce costs, risk, and potential legal liability; support innovation by offering standard platforms for development; and define and expand markets, and the value proposition associated with the market's products and services.

The effort to promote Identity Ecosystem interoperability internationally will in some ways be similar to the manner that interoperability is pursued in the global technical standard setting context. For example, technical standard development settings typically involve the establishment of a set of governance arrangements and intellectual property arrangements that support stakeholder consensus-based technical standards specifications that are enforced by mutual contract arrangements. Further, in technical standards setting contexts, governance varies depending on the particular setting, but typically

involves issues associated with voting, review and promotion of draft specifications, cost arrangements and the like.

In technical standard setting, intellectual property issues are typically associated with the three traditional pillars of IP: Patent, copyright and trademarks. Typical IP structures involve patent cross licensing (on RAND or FRAND terms); copyrights take the form of typically broad access licenses with respect to specifications; and the trademark issues are associated with the testing, certification, and marking arrangements associated with compliance with the specification. Governance and IPR are two of the major issues dealt with in technical standard setting.

*Governance of Legal and Policy "Rules" standard setting*

As suggested below, the current exercise in the context of data/identity markets is directed to a form of "standard setting." It is not just a different form of technical standard setting. It is, in fact, "legal" standard setting, aka rules setting, aka Trust Framework development. Since networked information systems depend on the reliable behavior of both technologies and people who handle data, we need to develop approaches that permit the normalization of both sources of system function at Internet scale. That will require standard setting relating to both technical specifications, and the rules that normalize human behaviors within those systems.

*"Legal" Standards Setting?*

Although it is infrequently recognized as such, legal standard setting is an area that has made possible massive benefits for social, commercial and governmental structures. The global financial markets, with all their recent challenges, have long provided examples of the benefits of standardization at scale. Nearly every financial instrument, derivative, payment transfer, loan, secured transaction, etc. is based on a legal form of "technical" standard. That "technical" standard is documented in the form of standardized contracts. For instance, the International Swap Dealers Association 1985 standard form launched interest rate swaps as a global market, as well as various iterations (currency swaps, etc.,). Each was based on a standard form of contract.

In the case of each such contract "standard," parties decide whether to "opt-in" to participation in the instrument, but to do so they typically need to accept the terms of the standard documents, with few or no changes. In the case of swaps, for instance, parties only "customize" agreements to the very limited extent of adding their names as parties, and including the interest rate and notional principal amounts and perhaps some contact information. The strength of these arrangements, and their ability to scale, is based on the fact that the parties are not invited to alter the standard document terms. Even though such restrictions may initially seem unfair, it is a small price to pay for the massive legal "network effect" make possible by standardized terms. Within the "community" of parties that have signed the same contract, behaviors are more predictable, reliable and even interoperable. Standard legal terms are a key to international interoperability for the Identity Ecosystem.

*What is the "low hanging fruit" of legal standardization at Internet scale*

In the present case, there are opportunities to identify elements of international networked information systems that may lend themselves more readily to standardization. For instance, it would seem that some more mechanistic aspects of system operation and administrative and operational elements will be more easily standardized across international systems.

The same is true of (legacy) system elements that depend on and are built around current commercial service offerings and terms, applied by market-leading entities, which establishes a form of *de facto* standardization, and elements of market inertia. Such standardization is also characteristic of elements of networked information systems that are subject to the laws and rules of those jurisdictions (such as those in the EU), that establish sets of duties and "standards of care" relating to various data handling activities.

*What is value proposition for "legal standards?"*

Standards define and drive markets, whether the markets are defined by value propositions from the technical side or from the legal side. The fundamental value proposition in the case of contracts is the ability to render the behavior of another legal actor (whether an individual or a legal entity) reliable, even in the absence of direct contract privity. That is it. In that sense, a contract is a "specification" for future action and behavior of the parties to the agreement.

*A contract says: "If X occurs, then you will do Y," and makes it enforceable*

Contracts make future behaviors of other legal persons more reliable and predictable. Now that we have constructed massively interoperable technologies to accommodate broadly interoperable data/information systems (that carry a variety of other commercial, governmental, and social systems), we need a similarly scaled set of "rules of the road" for behavior on these systems.

There are a variety of social "Rules" that affect the behavior of legal actors. The rules governing the behavior of legal entities (such as governments, companies, organizations and the like) are a bit more "formal" since those entities are created under legal fictions and so don't exercise the range of discretion in their behavior that is demonstrated by individual human actors (except by the fact that it is humans that act on behalf of such organizations providing the "agency" necessary to enable such discretion by a legal entity).

The more "mission critical" rules are written down in the form of laws, codes, contracts, regulations, etc. and other formal iterations of rules that sculpt behavior across social, political and commercial structures. Those formal "legal" rules are, in effect "standards" of behavior the presence of which has benefits similar to those established by technical standards.
The term "contract" as it is popularly understood suggests that it is an enforceable agreement. The presence of enforcement mechanisms in a contract is the equivalent of redundancy in engineered systems. It is an element of the system that increases the reliability of the system. In the case of agreements, legal actors are "caused" to act reliably through enforceable agreements.

*In law, "standards of care" inform legal duties*

The advantages of "standard setting" are not the exclusive province of technology. Standards have long been employed in policy and law to help differentiate system-consistent behaviors from undesirable behaviors that undermine system functions. Where there is a uniform set of duties or standards of care, it can result in substantial cost savings and efficiency gains within the jurisdiction(s) in which such uniform standards are applied.

The Uniform Commercial Code is an example of an intentional effort to derive uniform standards for various commercial practices in an effort to reduce the friction and costs associated with the mercantile economy taking place among the various U.S. states in the mid-20th century.

Where there are multiple, different "standards of care" imposed by different jurisdictions, it can have the opposite effect, making compliance more costly and less efficient. A recent example is presented by data security and data breach laws. Data breaches are quite typically caused by people issues, not technical issues. These "people issues" sometimes involve carelessness by data handlers and sometimes malicious acts by either insiders or external "hackers." Various states have passed laws to create duties and standards of care in an effort to curb these issues.

Data breaches do not all cause harm, but those that involve so-called "personal information" (as variously defined) could potentially result in the assertion of violation of various statutory duties of care. Where an activity is engaged in which covers multiple jurisdictions, inconsistent statutory duties of care between those jurisdictions can make compliance difficult or impossible. In addition, the same actions that can result in challenges under statutory duties of care can also potentially prompt examination under other common law standards of care, including those that inform the various notions of "privacy" as variously defined, in several common law traditions.[48] The challenges are even greater in the international context, where there are no baseline documents from which to build internationally interoperable standards of care.

It is the efforts to normalize various duties of care that are applied today that are the subject of the rulemaking activity that is the focus of current OIX efforts, and will be informed by the Steering Group work. To the extent that the Steering Group uses OIX programs and tools to help fulfill its mission, it will have greater access to international market information and developers.

The U.S. effort can also help to create globally interoperable systems that can address harms from either intentional or negligent causes. There are two chief sources of harm relating to Internet identity today: a lack of standards for people who want to do the right thing, and a challenge of addressing the system frailties in the face of intentional acts of theft and/or politically motivated actions.[49] Identity Ecosystem Framework standards can make progress in addressing both types of issues.

[48] For a chart that correlates various common law torts and their privacy related counterparts, and various fair information practice principles (that establish various statutory and/or regulatory duties of care in different jurisdictions), please see Exhibit C of the Respect Networks Corporation Trust Framework that is available at the OIX website at www.openidentityexchange.org.

[49] In the latter setting, to paraphrase Clauswitz, "*Hacking* is the continuation of politics by other means."

*Question 4.5: What is the Federal government's role in promoting international cooperation within the Identity Ecosystem?*

**Summary:**

The U.S. government's role will likely be similar to what it will be in the U.S. domestic NSTIC Identity Ecosystem; to support, convene, and to guide markets with the "power of the purse."

**Discussion:**

The Identity Ecosystem will mostly reflect the influence of market forces and private sector decision making. The U.S. government role will likely be similar to what it will be in the U.S. domestic NSTIC Identity Ecosystem. As in the domestic U.S. context, the U.S. government's role will be to support, convene, and serve as an early adopter.

One exception will be the limitation on its enforcement authority, as exercised domestically through the government's legislative, executive and judicial functions. The U.S. government frequently exercises its authority to support emerging domestic markets and socially and commercially desirable initiatives. Examples of similar situations include the passage of "Reg. E"[50] (that limits credit card and debit card holders' liability to $50, subject to certain statutory prerequisites.
The U.S. government will not have jurisdiction to exercise its enforcement authority in most international contexts. By contrast, within U.S. legal jurisdictional limits, one or all of the executive, legislative or judicial functions of government associated with enforcement might be called upon by the private sector to apply its enforcement authority to offer stability and certainty. This might include, for example, such system supporting exercises of authority as:

the passage of legislation establishing liability "safe harbors,"

from the executive branch, the issuance of regulations that are consistent with stakeholder consensus- based rules and clarify data handler duties of care reducing liability overhang,

from the judicial branch, more consistent treatment across state and federal court systems of current compliance requirements that will permit the creation of more effective Trust Frameworks to be built .

It is possible that incentives could be crafted that are based on system incentives and penalties but are indirectly supportive of international elements of data/identity markets and the networked information systems on which they depend.

[50] Reg. E is a reference to 12 CFR 205.

# PART II EXHIBITS

## 1.1.1A: Structuring to Address Complexity

*Complexity is a common stakeholder challenge*

System complexity is a challenge that all ecosystem stakeholders have in common. It is also a challenge for all governmental, commercial, community and other entities that seek to "govern" any parts of the ecosystem. The Steering Group should be structured to help all of these stakeholders deal with system complexity.

The Steering Group work on the Identity Ecosystem Framework should reflect current stakeholder needs, and also help to guide the natural growth of the market to address future stakeholder needs. It can do this through creation and continued maintenance of high level standards and principles that can support and inform private rulemaking activities (aka "Trust Framework development") all of which are directed toward streamlining uniform, integrated, multiparty contractual solutions (aka "Trust Frameworks") as a way of fostering interoperability and innovation to meet new system complexity challenges.

*Sources of complexity*

With its multiple stakeholders, broad range of contexts, myriad jurisdictions with multiple existing laws, and multiple industries and sectors each with both formal and informal traditions associated with data and information exchange, even getting a sense of the identity ecosystem, without even seeking to influence its direction, can seem overwhelming. In fact the complexity of networked data/identity systems, with their myriad interconnections, follows a power law growth curve, which tends to describe systems that quickly become "unmanageable" in the traditional sense of the word.[51]

*The challenge of maintaining "digital identity integrity" in a sea of data*

Within increasingly complex networked information systems, individuals and entities with legal capacity and/or legal rights need to be able to interact online for purposes of their respective data and identity integrity needs in ways that are reliable, predictable and interoperable and over which it is possible to preserve various forms of "digital identity integrity." Digital identity integrity is sometimes perceived

[51] The complexity of systems is frequently cited as the reason for a number of organizational and operational challenges, for example the "Iron Law of Oligarchy" applicable to bureaucracies, the "traveling salesman problem" associated with planning and logistics, and other similar complexity challenges.

and described as "privacy" (for an individual), or as "security" (for an individual or for a legal entity). Digital identity integrity is preserved to the extent that an individual or entity has more control over information inputs and outputs by and about them. The many different legal entities have many different needs, all of which they expect to be accommodated in data/identity systems that are presented for their use. They all have in common the need for some measure of "digital identity integrity."

*Using "Role-Based Modeling" to foster digital identity integrity*

Fortunately, there is something else that they have in common. It is the assumption of various generic roles within online data/identity systems as part of their ordinary interactions. It is therefore possible to describe generic "roles" that characterize the behavior of individuals and legal entities in different contexts, and thereby to simplify the analysis for modeling purposes.

These "roles" can, in turn, inform the composition of the categories to apply to the Plenary for purposes of establishing groupings that elect the governing board. Different roles generate different needs. Different needs should be represented on the governing board, even if substantial authority continues to reside in the plenary.

As always in modeling, care must be taken to ascribe characteristics to the roles (called "agents" in the models) that are appropriate for the particular person and model at issue, and agency-based modeling approaches that are thought to be less prone to overgeneralization should be considered.[52] Those same concerns should be addressed in the deliberations about which categories to apply to the Plenary for grouping stakeholders.

*Other sources of complexity: interconnection and context growth*

Even with the simplifications offered by various role modeling approaches, the situation is intrinsically complex as a direct result of the increased number of connections made possible with ever-advancing technology interoperability. In other words, even with a satisfactory roles list, the variety of contexts of interactions taking place over data/identity systems is also increasing exponentially.

*The legal lag*

Unfortunately, while the number of connections has increased along with greater technology interoperability, the "rules of the road" for people and institutions using networked information systems in myriad contexts have not kept pace. In fact, many anachronistic laws, regulations and even siloed, sectoral contract approaches to data/identity, seem frozen in time, like a deer in the headlights of change.

There are many reasons for this "legal lag," including institutional inertia, and because the mechanisms of changing the "rules of the road," i.e., legislation and regulation, were designed, sometimes intentionally, for a different pace of change.[53]

[52] See article in Science entitled "Pattern-Oriented Modeling of Agent-Based Complex Systems: Lessons from Ecology (Nov. 11, 2005) at http://www.sciencemag.org/content/310/5750/987.abstract?sid=cd0a3948-0503-425b-9e0d-cc03b5d15805

[53] A quick survey of U.S. federal law and EU directives reveals that nearly all were passed in the era prior to broad social networks, cloud computing and a host of other "networked information" innovations (see dates of statutes in Note 66.).

In the U.S., the concept of the "laboratory" of state laws in the federal system does not provide a solution; they merely add greater variety to the uncertainty, resulting in an exponential increase in compliance challenges, costs, etc. whenever they are encountered. Examples of the compliance variables include the nearly 50 different sets of state rules for online businesses regarding how they structure portions of their privacy policies, their data breach policies, sales tax and other local tax collection elements of online payment systems, and other requirements. The differences among different domestic and international jurisdictions' laws is another barrier to "legal interoperability."

*Contract as a source of "duty standards" to drive interoperability and reduce complexity*

As suggested below, legal duties can be created and documented either through public law (such as legislation and regulation) or by private contract. One approach to public law "lag and complexity" is to develop standardized contractual solutions to data/identity problems that can bridge jurisdictional and industry silos, and simplify complex systems. That is the essence of the Trust Framework development process and the broader Identity Ecosystem Framework process. OIX programs and tools are designed to support private and governmental sector Trust Framework development processes across jurisdictions and technologies. The Steering Group would benefit from using the same tools in its work.

*Plugging the Steering Group into emerging data/identity markets*

Since the Steering Group is intended to help promote standards for emerging data/identity markets, its governance should be structured to take maximum advantage of existing Trust Framework development processes, to support such processes, and to provide Trust Frameworks with the opportunity to earn a suitable "trust mark" or other indication of conformity to Steering Group-derived standards when that system is available. This provides a pathway toward standardization, i.e., by drawing voluntary participants into arrangements that have greater interoperability at the policy level as a result of being crafted around legal standards. The Participation Governance Model is intended to put the Steering Group in the position described above.

### 1.1.1B: Structuring to Address the Stakeholder Representation Issue

It is recognized that governance issues revolve around how individual entities (individuals, legal entities, etc.) get together to manage themselves, and typically also the mechanisms through which they each consent to be managed. Direct participation in all decision making does not scale, so representational systems (such as electing officials, etc.) are, of necessity, frequently resorted to for large systems. The global networked information system certainly qualifies as a large system.

One of the benefits of representative arrangements is that the delegation of authority for another person to act on your behalf can be efficient for the individual actor who can then leverage their activities into the broader system. The challenges arise in developing mechanisms that assure that the individual interests will be expressed in a fair and balanced way with other interests in the system, and that mechanisms will be made available to the individual entity to allow insight into decision-making processes, without requiring their full attention.

The issue of "participation" is further discussed in the "stakeholder participation" section of this Governance NOI response. For purposes of this structuring discussion, it is suggested that providing stakeholders with multiple pathways to participation can help to ease the challenges of representative governance structures. Stated more directly, the population of the Steering Group governance body will be less controversial if stakeholders have multiple effective pathways to participate in the rule making process. Also the open Plenary structure will have a similar effect. Part I describes the Participation Governance Model that is intended to support such a process.

The Steering Group governance structure should recognize the perennial challenges of "representation" (like elected officials) in scaled governance systems, and employ an open architecture, such as creation of an open Plenary with real authority and the application of the Participation Governance Model, that enables the Steering Group the market communication tools to most easily and efficiently interact with, receive input from, and provide input to a variety of different "influence nodes" within the ecosystem.[54]

It is recommended that those parties responsible for structuring the Steering Group avoid the understandable impulse to gravitate toward attempting a more "centrally managed" ecosystem, or to limit its information flow to that among the members of the Steering Group. The costs and challenges of an actively centrally managed approach might quickly outstrip any perceived benefit of seeking to aggressively "guide" the system. The greatest challenge may ultimately be the maintenance of authority of the Steering Group, i.e., the consent of the governed, if such an approach is pushed. These systems are voluntary, and will only be effective if adopted. The creation of effective information feedback loops between the Steering Group and the markets it is intending to affect is essential to its task.

[54] See "Controllability of complex networks" by Yang-Yu Liu, Jean-Jacques Slotine and Albert-Laszlo Barabasi in Nature, May 12, 2011 at 167 ("driver nodes" tend to avoid high-degree nodes, but can guide entire system dynamics in arbitrarily complex directed networks)

## 1.1.1C: Structuring to Address Decentralized Authority

The foregoing Exhibits discussed the challenges of interaction complexity and representation of large groups of stakeholders. This section raises the issues associated with governing intrinsically decentralized networks, such as globally networked information systems.

It is recognized that governance of the Steering Group is not the same as governing the ecosystem. It is however, also recognized that the Steering Group is intended to foster a form of self-regulation/self governance among stakeholders that will be "responsible" for governance of the ecosystem. Because of that connection, it may be useful to consider the challenges of governing the system (the "Identity Ecosystem") that is the ultimate object of the legal standards setting exercise that will be engaged in by the Steering Group and will inform its governance.

*Degrees of centralization of governance*

Governance models vary along many vectors. One important vector is the relationship of the governed and the governance structure. These relationships can be plotted on a continuum from more to less centralized. At the decentralized end of the continuum is self-governance, in which each stakeholder participates actively (but which doesn't scale very well). At the other end are various forms of autocracy, in which relevant decisions for the group are made by a single authority. In between lie a variety of structures where authority is more or less centralized.

*Decentralized systems: Decentralized governance*

It seems intuitive that effective governance of distributed systems will itself be distributed across such systems. That raises questions of how distributed systems can best relate to more traditional governance structures that were typically based on some sort of "centralization" around concepts of physical presence, nexus, permanent establishment, or other physical connection of person or entity to a geographic location and its associated legal jurisdiction. In the most extreme examples of disconnection, limited communities have sought to substantially reduce their ties to traditional legal jurisdictions in favor of alternative structures of self-governance that they proposed were more in keeping with their online values.[55]

*Layers of centralization in the U.S. system*

In the U.S. tradition, as in other forms of democracy, rules creation governance (aka politics and governmental systems) offer a compromise of a federated, representational democracy. That provides governance structures where some functions take place more centrally (in a federal governmental authority) and others more locally, such as that in state, county, city, town and other jurisdictional levels. The availability of more and less centralized layers of governance allows the assignment of governance sub functions to the most appropriate level.

*Steering Group centralization considered*

[55] In "Cypto Anarchy, Cyberstates, and Pirate Utopias," edited by Peter Ludlow (MIT Press, 2001) a number of articles explore issues associated with the implications for governance of decentralized structures of the Internet.

When considering the issue of how the identity ecosystem might sustainably operate (and be governed) from day to day (and by extension how the Steering Group governance structure should be constructed to support that operation (and governance)), one issue is whether the potentially appropriate models for ordering relationships should be more or less centralized. It is worthwhile to first consider the nature of the networked information system (aka the Internet) over which data/identity systems will be deployed.

*Decentralized information system yields distributed relationship structure*

The Internet was first designed to offer an information system that could be resilient against physical infrastructure attack associated with nuclear war and other similar scenarios. It achieved this, in large part, by utilizing a broadly distributed and redundant architecture. That resilience and adaptability has proven to be valuable in a number of settings.

As the Internet information infrastructure reflecting this distributed architecture is applied to support an increasingly broad range of legal persons' interactions, it should come as no surprise that such a broadly distributed architecture would yield a broadly distributed relationship structure, one that does not lend itself as readily to centralized governance. Challenges associated with financial and securities regulation, digitized intellectual property protection, regulation of gambling, money laundering and the prevention of terrorist group financing, are just a few examples of the new challenges of governance for activities in the decentralized Internet.

*The challenges of governance in a distributed relationship structure*

In fact, there are a multitude of legal standards and enforcement challenges that arise as a result of the fact that the distributed infrastructure provides options to participants to "work around" otherwise compulsory elements and controls. That is what the Internet was designed to enable. Now we must address the governance consequences of those earlier architectural decisions.

*Unpacking "governance" to allow tailoring of levels of centralization*

In evaluating the relative merits and benefits of centralized versus decentralized structures, it is worthwhile "unpacking" governance, to see whether certain aspects of governance might be gainfully treated differently than others in terms of their centralization. In other words, are some functions better "centralized" while others are better "localized?" Think of the questions asked when multiple hospitals share laundry services, or when companies outsource payroll services.

*Separating legislative, executive and judicial functions*

Governance can be viewed at the most general levels as composed of three basic functions that in the U.S. political system are associated with the legislative, executive and judicial function. Those basic functions characterize all governance, since even more autocratic structures engage in rulemaking, operations, and auditing even if without the discipline of "separation of powers."

If those three elements are typically present in governance structures, it may be fruitful to consider what distributed, decentralized, "crowd sourced" legislative, executive and judicial function might look like, and the degrees to which more or less centralization of each function is beneficial or detrimental to

the goals of NSTIC, and the work of the Steering Group. That may help to inform the types of structures that would benefit the Steering Group.

*Legislative function*

As a general matter, legislative activity is associated with rule making. In the Participation Governance Model, rulemaking authority associated with scalable, uniform Trust Frameworks resides in the groups that initiate each such Trust Framework development work, and in the individual rulemaking processes that they employ. In fact, under the OIX rules, each Trust Framework may draft its own charter, establishing governance rules that best suit its needs.

In the Participation Governance Model, rulemaking (legislative) authority for standardized contracts (that make up Trust Frameworks) also resides in the Steering Group(s), that establish higher level standards that act as a sort of filter for Trust Framework development, helping to guide that private development activity toward Steering Group-consistent goals.

Of course, the governments will also continue to have the ability to engage in rulemaking, through legislative processes that establish background law. In the name of interoperability, it is hoped that by providing access to OIX Trust Framework development tools and market information systems to all stakeholders, governmental and private, that both Trust Framework drafting and government legislative activity can be better coordinated, reducing compliance costs on both sectors. The work of the privately led Steering Group will help to bind these together.

Thus, it seems that legislative rulemaking activity will be somewhat decentralized going forward but that it can benefit from centralized resources to help guide those disparate legislative processes toward identifying multi-system "best practices" and toward the identification and development of candidates for standards that formalize those best practices. The Participation Governance Model relies strongly on the Steering Group to serve that centralized role within the overall decentralized rulemaking of the ecosystem, and relies on OIX programs and tools to provide the common platform for communication across current silos.

*Executive function*

The executive function of governance is associated with operation of the system, and executing the laws passed by the legislative function. It is also sometimes called upon to engage in rule development associated with operations, and consistent with the goals set forth in legislation/rulemaking. There will often be efficiencies associated with centralizing executive function, particularly where it is with respect to more ministerial, administrative and operational elements of identity ecosystem operations. It is easiest to centralize those types of functions that are more generic and less context driven, like the generic functions that can be more readily outsourced by a business (general accounting, payroll, tax return preparation, janitorial, etc.). In fact, the market for generic computing, data processing and other information processes has become sufficiently normalized that it is now increasingly "outsourced" by businesses and even individuals; and that outsourcing structure even has a name. . .the "cloud."

In the Participation Governance Model, there are several nodes through which the executive function is engaged. First, each Trust Framework initiative can independently decide how it wants its Trust Framework to be deployed and operated. They can decide what entity or entities will administer and operate the data/identity system that their Trust Framework describes. Another is the governance

board of the Steering Committee, which will perform certain assigned administrative and operational functions for the Steering Committee plenary.

*Outsourcing of generic functions drives interoperable rules*

It is anticipated that many Trust Framework initiatives will look to service providers to "outsource" or "cloud-source" many of the functions necessary to effectuate their Trust Framework, particularly the more administrative functions. Each such instance of such "outsourcing" provides an opportunity for system operational interoperability, particularly as standards are developed by and for the parties that provide such executive function services, and are captured in standard form contracts.

*OIX tools support operations and administration*

In support of Trust Framework development and the operation of orderly data/identity markets, OIX provides operational support for the information systems that are made available for Trust Framework development (the OIX Knowledge Center) and data/identity market operation (the OIX Listing Service). This is a form of sub-executive function directed at operating the "plumbing" for information relied on by other parties engaged in governance. OIX does not exercise any substantive control over the ultimate content of Trust Frameworks, it just makes them easier to deploy and operate at Internet scale.

*Judicial function*

The final sub-function of governance is "judicial," which in the case of data identity systems includes auditing and enforcement.[56] It is likely that there will be advantages in centralizing some of these functions for cost savings and for interoperability benefits.

Not all assessment, auditing and enforcement functions will be centralized. In fact, they cannot be all centralized due to the limitations of already strained central resources and the "power law problem."[57] Most incentive and penalty structures will be formulated more "locally" within each system, since these will likely be more effective and scale better. For example, if a local data/identity system operating under a particular Trust Framework establishes disqualification from using that service as a potential enforcement mechanism to enforce the performance of duties consistent with that Trust Framework, users of that system who value its use will more likely comply with the duties imposed by that system. That enforcement is entirely "local" and requires no outside enforcement mechanism.

The Department of Commerce Green Paper on privacy anticipates that industry-developed standards (standards associated with duties directed at providing individual data subjects with controls from which they can achieve their subjective level of "Privacy") can be enforced by the Federal Trade Commission. This is an example of how a division of legislative (private) and judicial (public) function can be unpacked to allow the benefits of both centralized and decentralized governance models.

[56] It is recognized that enforcement authority is also associated with the executive function, but that fact does not need elaboration for purposes of these illustrative categories of governance function.

[57] See footnote 53.

### 2.4.1: NSTIC Guiding Principles "Unpacking" Tool

The NSTIC and Governance NOI Guiding Principles are high-level statements of general system goals.

The NSTIC guiding principles specify that identity solutions must be:

Privacy enhancing and voluntary,
Secure and resilient,
Interoperable, and
Cost-effective and easy to use

Even though several of the principles are presented as "couplets" of two principles (e.g., secure and resilient), the entire set of principles includes 7 separate concepts, each of which warrants further "unpacking" in an effort to discern how duties might be constructed in open data/identity markets to cause systems to operate consistently with each such principle.

Putting in place processes that continually monitor and enable stabilized development of products and services to help define the nature of those duties, their specific "standards of care" and how they impact stakeholder behavior when handling and interacting with data in networked information systems is the essence of the NSTIC vision for an identity ecosystem.

Since there is significant subjectivity in the evaluation of the "achievement" of each of these principles, a substantial part of the Steering Group effort will be directed toward the discernment and balancing of various stakeholder group preferences (expressed through various market and voting mechanisms) to produce balanced, robust and flexible Identity Ecosystem standards that can help guide sustainable, normalized, reliable and interoperable markets that serve up products and services that fulfill the aspirations reflected in the principles.

The statement of these principles signals a significant maturation of the market and the analysis of networked information systems. This is because prior to their release, the public discussion of data/identity system requirements had focused mainly on the FIPPs, a set of "Fair Information Practice Principles" that are primarily (or solely) directed at the privacy interests of individual data subjects. This is understandable given that this particular focus was initiated and has been iterated by governments and government-led initiatives that seek to be responsive to those groups of stakeholders that influence decision making (mainly voters, but also other influencers).

As important as FIPPs based principles are (and their updated iterations will be very important to well functioning, scaled data/identity systems), they are only part of the story. The NSTIC Guiding Principles start to tell the rest of the story, one in which *all* stakeholders interests need to be addressed to build stable, self-sustaining systems and data and identity markets.

For example, the FIPPs say nothing directly about the needs and rights of non-individual data subjects such as companies or governments (although it seems clear that many of the FIPPs could also benefit such institutional data subjects). They also say nothing about the needs of relying parties or identity providers or other third party data handlers.

By contrast, the NSTIC Guiding Principles are substantially broader, dealing with issues such as system costs, user interfaces, sustainability and other issues that pick up where FIPPs leave off. The

incorporation of a broader, principle-based analysis of all stakeholder needs, as is initiated by the presentation of the NSTIC Guiding Principles, is a welcome and necessary step toward crafting more comprehensive integrated agreements, which will be more sustainable and cost effective.[58]

Like the FIPPs, the NSTIC Principles are crafted to provide high level guidance. They cannot be fully realized without greater specificity that can guide their expression in specific rules and structures, and that provide specific and enforceable benefits and rights to identified groups of stakeholders and impose corresponding specific duties and burdens on identified stakeholders. From this balance of rights and duties the principles are realized and the Identity Ecosystem based on those principles can be brought into existence.

This "Unpacking Tool" sometimes raises substantive issues that are beyond the scope of this Governance NOI response, which is why no attempt is made to provide a comprehensive treatment of these issues. The Tool provides a necessarily incomplete treatment of each of these important principles. Its chief deficiency is that it does not yet reflect the various views of stakeholder groups on the meaning of the stated NSTIC principles. That is work appropriately assigned to stakeholders, acting through markets and voting mechanisms made available through various Trust Framework standards initiatives and Steering Group initiatives, including the future work of the Steering Group plenary and its governance board.

Notwithstanding its intrinsic shortcomings, the tool is provided in this response for two reasons. To help to inform Steering Group governance structuring guidance by raising the particular unique aspects of the NSTIC principles substantive issues to be addressed by the Steering Group. For example, if it is observed that small business owners using online identity systems benefit from "Cost Effective" and "Easy to Use" identity systems, it may be viewed as important that small business owners be involved as Stakeholders in Steering Group Governance, and may suggest that testing protocols and objective criteria be developed with the involvement of these groups to identify conformance with these two principles as part of the Steering Group Rulemaking Process.

The substantive issues will be best developed by the Stakeholders themselves as part of the Governance Board design, development and operations. This initial version of the Unpacking Tool is not presented as a comprehensive treatment, but merely as a guide to a tool that might help in the current work to configure the Steering Group.

Second, the Unpacking Tool helps to point out the high level of integration and mutual dependency that will characterize stakeholder relationships in the Identity Ecosystem. For each person with "rights" in the system there must be a corresponding person(s) with a duty. Rights are irrelevant without assigning persons with a duty to respect them. What quickly becomes evident in the move from pre-market to structured market arrangements is that each stakeholder is willing to perform the duties in the system if they are therefore better able to enjoy rights that are of interest to them. The sustainability of the system will be based on expanding these rights/duties relationship beyond mere two party agreements,

[58] Please see discussion at response to question 3.1.2.The mutual exchange of promises can constitute contract consideration, so that more comprehensive structures involving greater diversity of stakeholders can provide a more cost effective solution that does not need to depend on monetary consideration to support performance of contractual duties.

but having Stakeholders recognize that their performance of duties supports the overall system from which they are able to enjoy specific rights.[59]

It is the overall comprehensive system of rights and duties, the "Identity Ecosystem" from which individual stakeholders can enjoy "network effect" benefits, not individual relationships. Two party relationships developed in isolation cannot achieve desirable scale in Identity Ecosystems any more than a single symbiotic, commensurate, mutual, parasitic, predator/prey or kinship relationship defines an entire biological ecosystem.

In this NSTIC Guiding Principles Correlator, each of the guiding principles set forth in NSTIC and Governance NOI can be seen as a basis for one or more sets of legal standards, built to conform to the guiding principle.

The Correlator sets forth the following for each NSTIC Guiding Principle:

> Brief suggestions for "unpacking" of the principle to inform Stakeholder discussions,
> Identification of Stakeholders that benefit (rights holders)
> Identification of Stakeholders that are burdened (duty obligors),
> Current related sources of authority (contract, statute, regulation, FIPPs, etc.)
> Answers to Governance NOI Questions 2.4.1, 2.4.2 and 2.4.3

[59] Consider for example that credit card holders enjoy "cost effective" and "easy to use" access to revolving consumer credit facilities through credit cards systems. The cardholders have "duties" to issuing banks through the card agreement, but don't have a direct pre-existing agreement with all the retailers who might accept the card. They enjoy the benefit of a "right" to use that system to pay for goods and services without elaborate one-to-one agreements (other than their cardmember terms).

**Guiding Principle – Privacy Enhancing**

1. "Unpacking" of the principle
What is Privacy? What is privacy enhancement?

Functional definition:
The term "privacy" is one of the most overused, ill-defined and volatile terms in the data/identity space. A full treatment (if one is possible) is certainly beyond the scope of this Governance NOI response. Solely for purposes of this first iteration presented as part of the draft "Unpacking Tool" we are applying a functional definition that "Privacy" is a shared desire[60] in a population to enjoy and recognize a right to be free from unwanted intrusions in both physical and information space. The presence or absence of "Intrusions" are to be defined by context and stakeholder needs. Under this definition, the absence of unwanted intrusions defines a state of privacy. The measure of the quantity of system control provided to a data subject (mostly through the adoption by data subjects of systems that also assign specific duties to others) to prevent unwanted intrusions has been proposed to be described as a "level of control" (LOC).

The duties imposed on each person to act in a manner that does not result in unwanted intrusions on others is the source of the "privacy" enjoyed by those that desire to avoid the unwanted intrusions. The nature of intrusion is changing over time as the concept of "identity integrity" is changing along with the ascendancy of the value proposition of digital identities maintained on networked information systems. A recent FTC staff report[61] speaks to this change in the nature of intrusion when it identifies unwanted intrusions as being among the chief categories of harm (along with personal injury and property damage) that were intended to be curbed in its traditional "harm's-based" approach to enforcement, while recognizing that the range of potential intrusions that cause harms is expanding, requiring a reexamination of the nature of intrusion and related harms.[62]

The "catalog" of potential intrusions" that are currently legally cognizable varies from one jurisdiction to another and in the U.S. is initially defined by traditional common and statutory law. If the law is to "keep up," the list will need to be continually updated as the set of possible interactions expands on networked information systems. As the range, variety and nature of interactions changes in networked information systems, so to will the idea of identity "integrity" (the ability to maintain an identity boundary or membrane to suit one's needs in a sea of data), and the concept of intrusion on that changing "integrity." Both the intrusion and the integrity are subjective states of mind that need to be developed into more objective and scalable standards through the modern equivalent of a "reasonable expectations" type test, geared to various contexts. Acting in a way that is consistent with the

[60] Daniel Solove has proposed, in the interest of fostering a more balanced discussion of social goods, that privacy be treated as a commonly-held desire to be free from various forms of unwanted intrusion, and not as an individual expectation. For a discussion of some of the policy implications of that view see, http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/

[61] The FTC Preliminary Staff Report entitled "Protecting Consumer Privacy in an Era of Rapid Change" cites three types of harms that have traditionally been identified including harms to person, harms to property *and intrusion."*

[62] Id. at pages 9 and 20.

"reasonable expectation" of other parties to access information will not be deemed an intrusion, and a "reasonable expectation" of identity "integrity" will be defended against unwarranted intrusions.

2. Stakeholders that benefit (rights holders)

Privacy is broadly considered to be of benefit to individual, human data subjects. It is rarely, if ever, asserted that a legal entity (such as a corporation or government entity) has a right to "privacy."

Importantly, however, the same notions of "identity integrity" and "intrusion" that apply in analyzing "privacy" can also be applied to evaluate many aspects of the concept of "security," which is of great interest to companies and governments, who must protect their confidential and proprietary information against unauthorized access and other intrusions, and who must themselves understand and discharge their duties to protect the data with which they are entrusted in order to avoid liability for failure to comply with data security laws.

3. Stakeholders that are burdened (duty obligors)

Once "privacy is seen as the ability to reasonably control against intrusion, it is possible to conceive of the parties to be burdened by legal duties as those parties that are in a position to prevent such intrusions, in accordance with specific objective rules that establish their duties to so act. This includes data collectors, handlers and others such as relying parties (pursuant to integrity-providing "relying party best practices,"), identity providers that collect data from data subjects, and even third party behavioral advertisers that reconstruct identities and/or assign attributes from various pieces of innocuous, non-identifying data[63]

4. Current sources of authority (contract, statute, regulation, FIPPs, etc.)

Without going into too much detail about the current privacy-related "catalog of intrusions" in the U.S, .a summary listing may help to identify some of the core types of intrusions, the duties to be assigned to prevent those intrusions, to whom they would be assigned, etc. These include:

Common law: Tort of misappropriation of name/likeness (based in infringement and conversion)
Tort of "invasion of privacy" (based in trespass)
Tort of publication of private facts (reputational harm)[64]
Tort of defamation (false light, reputational harm)

Statutory Law: Many statutes that are broadly seen as "privacy-related" do not provide additional definitions of privacy, but instead establish duties for third party data handlers to do certain things. These things might include providing notice of data policies and receiving consent to data terms, providing notice of a data breach event, taking steps to dispose of data properly, reasonably protecting data in a variety of settings, etc.

[63] In the latter case, the event that takes place when the identity is "recreated" from such data can be called the "recognition event, and the occurrence of a recognition event may be viewed as a time at which some duties and privacy rights could each "spring" into existence. It is objectively testable and, because it requires a party to have engaged in the reconstruction of identity, it provides a legal party to whom the duties can be assigned.

[64] Helen Nissenbaum has described these concepts in the related surveillance context as "contextual appropriateness" and "distribution norms."

In a sense, those third party duties indirectly define privacy (or more typically some form of data security) by defining what other parties are obliged to do to the benefit of data subjects generally, which indirectly benefits a particular data subject. In a similar way, most FIPPs principles, whether codified in law or not, do not define "privacy," but also establish duties of data collectors and handlers.[65] The performance of these duties in conformity with the various sets of similar principles gives rise to greater data subject "control" of data, even when the data is not in the possession of the data subject.

By providing data subjects with the "right" to have these third party duties performed on their behalf, with respect to data about them held by such third parties, the data subjects are provided with the "levers" that enable them to achieve their desired level of control. More importantly, the provision of such controls to data subjects, with the enablement that they can each then use the controls as they see fit, is a mechanism through which various subjective perceptions of "privacy" can be accommodated in broadly standardized systems.

5. (Governance NOI Question 1.7 ) To what extent can each of the Guiding Principles of the Strategy-interoperability, security, privacy and ease of use—be supported without risking "pull through" regulation from regulated participants in the Identity Ecosystem?

This question invokes an involved analysis, since most "regulated participants" in the Identity Ecosystem will be subject to specific rules relating to "data security" which is not identical to, but related to "privacy." The ultimate resolution of these issues will be appropriately pursued by the Steering Group plenary and will involve understanding and separating "privacy" needs from data security needs in each separate data regulated context.

For example, in the data-regulated financial sector, it would seem like theft of money from a bank account that was affected through the criminal, unauthorized use of the identity credentials of the victim would involve a data security incident, but not a privacy incident. The harm is economic. The instrumentality of the crime, i.e., the financial account data, may be classified as "personal information" under various statutes, but there is nothing about an "account number" and password that is intrinsically personal. The harm seems more a harm against property than one of privacy or identity intrusion, per se. These distinctions are currently underdeveloped, and will benefit from examination and potential standardization by the Steering Group, since clearer definitions will help to clarify third party duties..

6. (Governance NOI Question 2.4.1) Do certain methods of establishing the Steering Group create greater risks to the Guiding Principles?

The methods of establishing the group would not appear to directly affect whether the solutions in the Identity Ecosystem are privacy enhancing. As long as the stakeholder representation includes parties who can speak to the privacy issues and how they might be addressed at scale, it would seem that the Steering Group could appropriately address the issues.

7. (Governance NOI Question 2.4.2) What measures can best mitigate those risks?

Use of the OIX risk wiki as a platform for the continuous development of the various sub-issues raised by privacy considerations can help to develop the issues to the point where they can be more readily operationalized through detailed treatment of duties in Trust Frameworks.

[65] For a list of the duties that arise under 17 separate set of FIPPs principles, sorted by type of duty, please see the link to the OIX FIPPs Comparison Tool at http://openidentityexchange.org/working-groups/legal-analysis .

8. (Governance NOI Questions 2.4.3) What role can the government play to help to ensure the Guiding Principles are upheld?

There are generally two institutional sources of potential "intrusion" recognized by individuals and cited by privacy advocates as being of potential concern. These include intrusions by commercial interests and intrusions by governmental interests. They share similarities, but are also different. These cover intrusions experienced in the commercial and political/civic spheres. It is certainly possible to conceive of a third category of intrusions in the social sphere, but these will typically occur as the result of the behavior of individuals, rather than institutions, and hence will likely invite a somewhat different analysis.

The government has at least two different roles to play in the two types of potential institutional intrusion. It is an advocate for individuals and other entities as consumers in the commercial setting where the perceived intrusions can occur as a result of the actions of commercial stakeholders. Separately, the government can be seen as the source of the intrusion where the government itself is interacting with individuals. In either event, the government can play the role of stakeholder in the Steering Group and of active contributor to the OIX online development tools to help develop these issues further to provide greater clarity on the dividing line between interaction and intrusion with respect to individual identity integrity in various commercial and governmental contexts.

**Guiding Principle – Voluntary**

1. "Unpacking" of the principle,

"Voluntary" means non-compulsory. Having said that, there are multiple types of compulsion. It seems that the principle here is that all stakeholders have the choice of whether to participate in the system.

Voluntariness is particularly challenging when system "network effects" become sufficiently attractive that the benefits to stakeholders become irresistible. In this case, it is still presumed that the decision to join represents an exercise of discretion and a decision taken through free will by the stakeholder. Such a decision would appear to still be voluntary.

It is not only desirable that participation in the Identity Ecosystem be voluntary, it may simply be necessary that it be so. This is because, as noted elsewhere in this text, Internet-scale systems are not confined to use or operation in a single legal jurisdiction. As a result it is more difficult for sovereigns and other traditional legal authorities to compel participation in Internet based systems using traditional means.

Instead, international systems will be based on contract, and contracts can only be formed by mutual volitional acts. A compelled "agreement" is typically voidable *ab initio;* it is deemed to never have been formed.. International iterations of Identity Ecosystems will be built on voluntary contracts.
Having said that, a distinction should be made between participation, which is voluntary, and following the rules of the system (consistent with the Identity Ecosystem Framework) which is mandatory. Once the voluntary decision is made by a stakeholder to participate, their behavior in that system must be consistent with the common rules.

2. Stakeholders that benefit (rights holders)

All stakeholders benefit from voluntary, contractual systems since they intrinsically allow for choice, the exercise of discretion and the opportunity to evaluation relative benefits and act on them can broadly be considered a form of "negotiation." In formal contract terms, each product and service made available might be considered an "offer" which upon "acceptance" forms a contract. Sometimes that negotiation takes the form of active discussion of terms, while at other times it takes the form of a unilateral consumption decision (which service to use), in a well functioning market that presents several alternatives from which stakeholders can make choices.

3. Stakeholders that are burdened (duty obligors), and

It is anticipated that the data/identity market in which stakeholders exercise their voluntary choices will be characterized by multiple Trust Frameworks operating at different levels to serve up reliable data/identity "rights" in the form of various LOA, LOP and LOC-based products and services. For each data/identity right, there is a corresponding duty. Thus, just as all parties will benefit from such contractual arrangements, all will also be burdened by such arrangements. Each stakeholder in each role will need to make decisions based on both the benefits and burdens of each such product or services. The data/identity service consumption decision will be similar to that made by a credit card customer that shops for both features (rights) and requirements (duties) of different cards, or a person shopping for a mortgage may look to not just the amount borrowed (rights), but the relative burdens imposed in the form of different repayment duties by different banks.

4. Current sources of authority (contract, statute, regulation, FIPPs, etc.)
The freedom to enter into voluntary agreements is a broadly recognized (although perhaps not universal) right. While such things as the default rules, consumer protection rules, contract formalities and other rules may vary from one legal jurisdiction to another, the establishment of Internet scale norms for voluntariness of data/identity related agreements is expected to arise.

5. (Governance NOI Question 1.7 ) To what extent can each of the Guiding Principles of the Strategy-interoperability, security, privacy and ease of use—be supported without risking "pull through" regulation from regulated participants in the Identity Ecosystem?
The notion of a "data-regulated" participant may be fundamentally inconsistent with the notion of voluntariness. For instance, in the U.S. certain entities (such as those involved in healthcare, financial work, education, etc.) are required, as a matter of law to comply with one or another of the various data laws. Their participation is compulsory, not voluntary.

Having said that, regulated participants are not compelled to adopt those solutions that are outside of those required by applicable law. Thus, for example, a business subject to the specific requirements of financial data regulation might make independent decisions about other aspects of their data handling systems, as long as those are not inconsistent with their performance of the regulated activities. Thus, they can still adopt non-compelled solutions voluntarily. The duties placed on different sectors of regulated data participants (healthcare versus financial, etc.) may vary, with corresponding different challenges of "pull through" regulations for each.

6. (Governance NOI Question 2.4.1) Do certain methods of establishing the Steering Group create greater risks to the Guiding Principles?
The manner in which the Steering Group is initiated would not seem to directly affect whether the solutions are voluntary. As noted elsewhere in this response, a private sector led initiative with broad stakeholder representation will be more likely to propose solutions that will be broadly viewed as favorable, increasing voluntary adoption, but the quality of the representation in the group is not driven solely by the methods of establishment of the group.

7. (Governance NOI Question 2.4.2) What measures can best mitigate those risks?
See above. Emphasizing the contractual nature of Trust Frameworks will help to confirm the point that solutions need to be voluntary. The OIX Wiki and other Trust Framework development tools help stakeholders to "unpack" their respective burdens and benefits associated with a particular data/identity solution, which can help to inform their voluntary decision on whether to participate.

8. (Governance NOI Questions 2.4.3) What role can the government play to help to ensure the Guiding Principles are upheld?
The government can participate as a stakeholder in Steering Group discussions. It can also contribute to the OIX online "conversation" to help develop the issues for consideration by other stakeholders.

**Guiding Principle - Secure**

1. "Unpacking" of the principle

Like privacy, "security" is a term that is applied in multiple contexts, making meaning more difficult to discern. The dictionary definition includes helpful notions such as "to make safe" and "to put beyond the hazard of losing or of not receiving." The notion is clearly affected by context and expectations. In all cases, however, there is a common theme of reliability, predictability and certainty that is understood to be present in addressing whatever harm is intended to be avoided with such security.

To the extent that privacy is defined as arising from data subject control, it may be that many of the same controls that are made available to stakeholders to help them experience their desired level of privacy will be the same as those that can potentially enhance security. This is not to say that the two are synonymous; they are not. It is likely, however, that some solutions will find application as both "privacy" and "security" enhancing.

There are at least two basic types of harms that are addressed in secure systems. These are harms caused by intentional third party acts, and harms caused by negligence (either of third parties, or other the party experiencing the harm). Legal and technical standards can help to mitigate both potential sources of harm.

2. Stakeholders that benefit (rights holders)

All stakeholders (other than unauthorized users and perhaps stakeholders in the business of selling insurance coverage for cyber risks and losses) benefit from secure solutions. Secure solutions are less prone to unauthorized access and other intentional behaviors, which means they are more predictable and less costly. They are also less prone to losses due to negligent behavior.

3. Stakeholders that are burdened (duty obligors), and

In security, it appears that the weakest link will be subject to potential exploitation by unauthorized users. In networked information systems, there are many potential links in how data moves, and just as many potential points of failure. Therefore, system security will be best configured at the system level, rather than merely focusing on individual stakeholders. In this context, the standardized duties of common contracts that are consistent with Trust Frameworks that are themselves consistent with the Identity Ecosystem framework can help to render stakeholders' duties consistent across systems, with corresponding system-scale benefits.

4. Current sources of authority (contract, statute, regulation, FIPPs, etc.)

There are several dozen U.S. federal statutes that impose various duties associated with data security and related issues.[66] Most reflect efforts to curb perceived harms in a particular context, and nearly all

[66] *American Recovery and Reinvestment Act of 2009 (ARRA*), Pub. L. 111-5, Title XII, Subtitle D – Privacy (ARRA)(health records data breach notice); *Cable Communications Policy Act of 1984*, 47 U.S.C 551, 47 U.S.C 421-573 (need consent to collect cable consumer buying habits data); *Census Confidentiality Statute,* 13 U.S.C 9 (census data use limitation); *Children's Online Privacy Protection Act,* 15 U.S.C 6501, et seq.(protection of children's data); *Computer Fraud and Abuse Act,* 18 U.S.C 1030(authorizes private right of action for unauthorized computer access or transmission); *Computer Matching and Privacy Protection Act of 1988,* 5 U.S.C 552(o)-552(q)(limits data matching by federal agencies); Confidential Information Protection and Statistical Efficiency Act of 2002, Public Law 107-347 (2002), § 501-526 amending 42 U.S.C 3501(limits federal executive agencies disclosure of certain confidential information); *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* (CANSPAM), Pub. L. No. 108-187 (2003) (CANSPAM)(regulating intrusion of commercial e-mails); *Driver's Privacy Protection Act of 1994,* 18 U.S.C 2721 (limits use of personal information in state driver records); 42 U.S.C 405(c)(2)(C)(vi)(prohibits states from

were passed at a much earlier stage of development of networked information systems. Thus, while they together describe the overall regulatory landscape, each of their respective "solutions" should be closely examined to discern whether it is consistent with current stakeholder needs before it is iterated more broadly as a system solution.

5. (Governance NOI Question 1.7 ) To what extent can each of the Guiding Principles of the Strategy-interoperability, security, privacy and ease of use—be supported without risking "pull through" regulation from regulated participants in the Identity Ecosystem?

As noted above, and as listed in the footnotes, there are a host of federal laws that define specific stakeholder duties associated with data in different contexts. This appears to give a sense of the group of "regulated participants" referred to in the question. Notably, the legal presumptions and paradigms applied in other jurisdictions may substantially increase the pool of the "regulated participants" (to include all personal data handlers) mooting the question in those jurisdictions.

As suggested above, some subset of solutions that are currently applied to regulated participants may be gainfully explored for application in the Identity Ecosystem, but that should not be assumed merely by their current application in law. Where those same or similar requirements are applied (for example at higher LOA and LOP levels), "pull through" will not be a problem, but rather an interoperability opportunity.

---

putting SSN on drivers licenses), But see The REAL ID Act of 2005, P.L. 109-13, § 201 et seq. (2005)(which requires states to verify personal information before issuing drivers license acceptable at federal facilities); *Electronic Communications Privacy Act,* 18 U.S.C 2510 et seq.(regulates access to stored communications and meta data about system use); *Electronic Fund Transfer Act,* 15 U.S.C 1601 et. Seq.(requires electronic fund transfer contracts to disclose when consumer information will be disclosed); *Employee Polygraph Protection Act,* 29 U.S.C § 2001(limits use of lie detectors by employers); *Fair Credit Reporting Act,* 15 U.S.C § 1681-1681(regulates use of consumer reports); *Family Educational Rights and Privacy Act,* 20 U.S.C 1232(g) and 34 CFR 99 (limits disclosure of educational information); *Federal Communications Act*, 47 U.S.C 222; 47 CFR 64.2001 (limits disclosure of CPNI); *Federal Information Security Management Act of 2002 (FISMA)*, Title III of the E-Government Act of 2002, Pub. L. No. 107-347(federal agencies must implement procedures to respond to data security breaches and implement NIST guidelines); *Section 5 of the Federal Trade Commission Act,* 15 U.S.C 41 et seq.(provides FTC with authority to address unfair and deceptive business practices); *Genetic Information Nondiscrimination Act of 2008,* P.L. 110-233 (5/21/08), 122 STAT. 881(genetic information protections); *Gramm-Leach-Bliley Act*, 15 U.S.C 6801-6827 and 16 CFR Pt. 313(financial information); *Health Insurance Portability and Accountability Act of 1996*, 42 U.S.C 1320; 45 CFR Pts. 160 and 164(health data); *Health Research Data,* 42 U.S.C 242m(restricts disclosure of national health statistical data); *IRS Disclosure of Tax Return Information,* See 26 CFR Parts 301 and 602, 68 Fed. Reg. 22596 (4/29/03)(consent for tax return disclosure); *Mail Privacy*, 39 U.S.C 404c (prohibits opening of sealed mail; *Telephone Records and Privacy Protection Act of 2006*, PL 109-476, 2007 HR 4709(prohibits obtaining phone records through pretexting); *Paperwork Reduction Act of 1980,* 44 U.S.C 3501, et seq.(prohibits federal agency collection of duplicate information from public); *Privacy Act of 1974,* 44 U.S.C 3501, et seq.(limits federal government disclosure of personal information); *Privacy Protection Act,* 42 U.S.C 2000aa(a)(b)(prohibits police search and seizure of documents intended for publication); *Private Security Officer Employment Authorization Act of 2004*, See § 6402(regulates background checks on employees performing security functions); *Public Health Service Act,* See § 308(d) of PHSA, codified at 42 U.S.C 242m(protects privacy of individuals in research data); *Paperwork Reduction Act of 1980,* 44 U.S.C 3501-3520(federal information policy); *PROTECT Our Children Act of 2008,* P.L. 110-401 (10/13/08); a/k/a Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008; Amending 18 U.S.C 2258 to add 2258A; See also 18 U.S.C 2258B and 18 U.S.C 2258C(prevent online child exploitation; *Right to Financial Privacy Act of 1978,* 12 U.S.C 3401-3422(protect financial information held by banks from government access); *Video Privacy Protection Act of 1988,* 8 U.S.C 2710 et seq. (protects video rental records; *Violence Against Women and Department of Justice Reauthorization Act of 2005,* PL 109-162 (HR 3402)(1/1/06)(privacy protection for domestic violence victims).

6. (Governance NOI Question 2.4.1) Do certain methods of establishing the Steering Group create greater risks to the Guiding Principles?
It does not appear that the method of the establishing the Steering Group will directly affect the quality of security-enhancing solutions.

7. (Governance NOI Question 2.4.2) What measures can best mitigate those risks?
Not applicable.

8. (Governance NOI Questions 2.4.3) What role can the government play to help to ensure the Guiding Principles are upheld?
As with the other guiding principles, the government can best participate as an active stakeholder in the Steering Group activities and in the ongoing discussion and development activity online.

**Guiding Principle – Resilient**

1. "Unpacking" of the principle

Resilience suggests an ability to recover from change. As the presence of change (and its increased pace) is the one data/identity market variable that won't change, resilience is critical.

For solutions to be resilient, they must either change along with the problems to which they are directed, or must themselves be directed toward reducing the pace of change in a particular context (by temporarily "freezing" interaction rules by mutual agreement of the affected parties).

2. Stakeholders that benefit (rights holders)
All stakeholders will benefit from resilient systems, since they will be able to more reliably deliver solutions even as conditions change.

3. Stakeholders that are burdened (duty obligors), and
Obligors may be challenged to satisfy some of the duties that are imposed by resilient systems. In the case where the solutions are resilient because they keep up with change, obligors will be asked to repeatedly change their operations to accommodate such continuously changing duties. This will be more costly for such obligors.

In the other situation, where change is managed by creating solutions that seek to reducing the pace of change (such as setting standards even as the area changes), obligors will be asked to maintain systems even though other external elements continue to change. This may put a strain on obligors as frozen standards increasingly diverge from changes external to those standards.

Because many data/identity legal solutions will depend heavily on the performance of duty obligors, the challenge of defining Identity Ecosystem standards will be to identify standard duties that stakeholders can continue to adhere to, even as change takes place. The most effective mechanisms for achieving this will rely on the stakeholders themselves to help configure systems, and will require strong communications to and from stakeholder groups to create the information feedback needed to configure these systems.

4. Current sources of authority (contract, statute, regulation, FIPPs, etc.)

5. (Governance NOI Question 1.7 ) To what extent can each of the Guiding Principles of the Strategy-interoperability, security, privacy and ease of use—be supported without risking "pull through" regulation from regulated participants in the Identity Ecosystem?
To the extent that resiliency is equated with the ability to respond to change, regulated participants may find themselves at a disadvantage if the laws to which they are subject are "frozen" relative to a changing market. Question 1.7 did not call out the "resiliency" principle specifically, so it is not clear whether the "resiliency" principle was intended to be covered in that question.

In order to support reliability of systems in regulated data settings (such as financial or healthcare, etc.), it will be helpful to maintain some consistency through time. While this continuity is desirable from a stakeholder perspective, it is challenging for policy makers who want to address current stakeholder

needs as those needs change. In that context, it will be useful to establish whether solutions are "comparable," rather than requiring them to be "identical," as a way of bridging the gap.

6. (Governance NOI Question 2.4.1) Do certain methods of establishing the Steering Group create greater risks to the Guiding Principles?

The NSTIC recognizes that private sector leadership in the Steering Group will result in the most effective governance structure. That recognition is based, at least in part, on the understanding that the private sector will be able to more nimbly respond to change. Therefore, those approaches to establishing the Steering Group that foster private sector leadership will likely be most able to avoid risk to the sustainability principle.

7. (Governance NOI Question 2.4.2) What measures can best mitigate those risks? See above.

8. (Governance NOI Questions 2.4.3) What role can the government play to help to ensure the Guiding Principles are upheld?

The government can most effectively take the limited role suggested in the NOI.

**Guiding Principle – Interoperable**

1. "Unpacking" of the principle

Interoperable systems have a number of benefits including cost savings, innovation and market expansion opportunities, easier UIs, higher security (through the "neighborhood watch" effect and because they are less easily phished or "pre-texted" by third parties), etc.

Interoperable systems depend on standardization of those elements that are to serve as the "points of connection" between and among systems. There will be many such points, some of which will be based on technical standardization (documented in specifications and patent cross licenses) and legal standardization (documented in contracts and laws).

Within the basket of "technical tools and legal rules" from which data/identity systems are constructed, a subset of those tools and rules will be standardized (and hence made interoperable) among the systems that are used by various stakeholders.

2. Stakeholders that benefit (rights holders)

All stakeholders enjoy the benefits of interoperability (other than those that currently depend on the maintenance of proprietary systems). Notably, even stakeholders that rely on proprietary systems to maintain confidentiality, secrecy, market share, etc., can benefit from interoperability of data/identity system elements that are consistent with their respective proprietary interests.

3. Stakeholders that are burdened (duty obligors), and

It may be that it is the providers of services and products for data/identity systems that are the most burdened by interoperability duties, since it is their products and services that need to conform to standards, which limits their freedom to alter their design and function.

Having said that, when it comes to "legal standards" and the duties that they create, any stakeholder may be potentially required to comply with the standard, depending on the context in which that particular interoperable variable is intended to be present. Thus, for example, a data subject supplying data that is intended to be made available interoperably across several sectors may be required to present that information in a certain format, or to engage in certain additional credentialing ceremonies to support authentication associated with that data in multiple sectors, etc.

4. Current sources of authority (contract, statute, regulation, FIPPs, etc.)

"Legal interoperability" is created when there are uniform duties imposed across populations. There are two general sources for duties; public law (statutes, regulations, cases) and private law (contracts).

Public law is compulsory across the affected population. It is a form of *de facto* standardization within a legal jurisdiction that results in interoperability. The downside of using laws, regulations, and other sources of public law as the source of standardization is that it is slow to respond to change, and may not reflect the interests of stakeholders most affected by the law.

Duties established by contract are often viewed as the preferred vehicle for achieving interoperability. First, they are voluntary rather than compulsory. Second they are quickly put together and can be more readily modified to respond to change. There are multiple examples of the use of contracts to create uniform duties to establish and maintain B2B identity authentication systems. The payment card

systems (and their PCI-DSS standard) is an example of a more broadly applicable standard for identity based transactions.

5. (Governance NOI Question 1.7 ) To what extent can each of the Guiding Principles of the Strategy-interoperability, security, privacy and ease of use—be supported without risking "pull through" regulation from regulated participants in the Identity Ecosystem?

To the extent that regulated data participants are forced to continue to conform to data regulations, they might be challenged to resolve the requirements that are placed on them by such regulations with those that would be more interoperable with other systems where those regulations don't apply. Those challenges will not be present in those areas that are beyond the scope of the applicable regulations. Regulated participants will not be at an interoperability disadvantage in those out of scope areas.

The comparability analysis described above may help to mitigate this problem.

6. (Governance NOI Question 2.4.1) Do certain methods of establishing the Steering Group create greater risks to the Guiding Principles? Not Applicable

7. (Governance NOI Question 2.4.2) What measures can best mitigate those risks?
Unpacking of current specific requirements that are imposed on regulated participants may help to identify which requirements would be more or less amenable to being made interoperable with those of other systems.

Even with mandated solutions for a particular regulated sector, interoperability may be pursued through the use of "comparability" analysis among solutions or through the migration of some subset of standardized solutions toward those applied in the regulated context. As an example of the latter point, some of the processes for authentication applied in a particular regulated context might be applied (directly or through a "normative cross reference) for some of the higher levels of assurance (LOAs).

8. (Governance NOI Questions 2.4.3) What role can the government play to help to ensure the Guiding Principles are upheld?
The government can avoid passing legislation or regulations without consulting with the private sector to assure that it does not further perpetuate sectoral differences that undermine interoperability. The government can also work with the private sector to discern whether there are agreed upon legislative or regulatory actions that might be taken, in furtherance of the standards created by the private sector that can help to drive interoperability (such as Reg. E did for the payment card industry).

**Guiding Principle – Cost Effective**

1. "Unpacking" of the principle

The cost effective principle is fairly self explanatory. Importantly, cost effectiveness is somewhat subjective and contextual, and so may be difficult to generalize.

2. Stakeholders that benefit (rights holders)

All stakeholders benefit from cost savings.

3. Stakeholders that are burdened (duty obligors), and

Arguably the party providing the service and getting paid (or foregoing payment) is the party burdened by cost effective systems. Having said that, stakeholders providing solutions can be expected to act in their self interest, and are therefore unlikely to provide solutions for which the burdens outweigh the benefits to them.

4. Current sources of authority (contract, statute, regulation, FIPPs, etc.)

5. (Governance NOI Question 1.7 ) To what extent can each of the Guiding Principles of the Strategy-interoperability, security, privacy and ease of use—be supported without risking "pull through" regulation from regulated participants in the Identity Ecosystem?

Parties that are subject to data regulation likely will incur costs associated with that compliance. For such companies, being subject to an additional, overlapping and possibly contrary set of duties under a Trust Framework may substantially increase their costs.

6. (Governance NOI Question 2.4.1) Do certain methods of establishing the Steering Group create greater risks to the Guiding Principles?

The manner in which the Steering Group is established will affect the cost effectiveness of the Steering Group operations, but appears less likely to affect the cost effectiveness of proposed solutions.

7. (Governance NOI Question 2.4.2) What measures can best mitigate those risks?

The OIX tools are intended to foster open communication about open standards toward creation and maintenance of open, competitive markets in which innovation and competition can help to drive down costs. Affirmative efforts to develop those tools and resources will help to achieve those markets and to keep costs down.

8. (Governance NOI Questions 2.4.3) What role can the government play to help to ensure the Guiding Principles are upheld?

Participate in the development activities as a stakeholder and user of solutions.

**Guiding Principle – Easy to Use**

1. "Unpacking" of the principle

Ease of use can be driven by various factors. User interfaces can be made simple to make applications easier to use. Also, the adoption of standards can help make applications easier by permitting them to be more familiar to end users (since learning one solution automatically provides awareness about the operations of other interoperable solutions).

2. Stakeholders that benefit (rights holders)

While ease of use if most often noted as desirable to individual stakeholders, it is clear that all stakeholders benefit from ease of use. Even institutional stakeholders depend on individuals to engage with data/identity systems on their behalf (whether as employees, independent contractors, etc.), so that more human friendly UIs will benefit all stakeholders.

3. Stakeholders that are burdened (duty obligors), and

The implementation of the ease of use principle would not appear to burden any particular stakeholder with a duty, other than perhaps the developers of such systems during the stage of development. To the extent that ease of use is accomplished by making the system rules more simple/standardized for all stakeholders that handle data, that will require the same broad creation and enforcement of duties across stakeholder groups as is required for several of the other solutions listed.

4. Current sources of authority (contract, statute, regulation, FIPPs, etc.) Not applicable

5. (Governance NOI Question 1.7 ) To what extent can each of the Guiding Principles of the Strategy-interoperability, security, privacy and ease of use—be supported without risking "pull through" regulation from regulated participants in the Identity Ecosystem?

As was the case with other responses to question 1.7, to the extent that there is a distinction between the duties imposed under data regulations and the duties imposed under an Identity Ecosystem framework standard, it will likely make it more difficult for such regulated participants to comply with either system. This is true whether or not the solutions are recognized to be easy to use, and it results from the potential risk of inconsistent requirements being placed on a single entity.

It is possible that some regulated participants may choose to continue to use an existing solution, even if it is not as easy to use as a new solution, as the result of legacies, dependencies, etc. As was noted above, a comparability analysis may help to reveal those situations where one or another solution can be chosen in the discretion of the stakeholder, to help preserve ease of use, and to allow for the more gradual transition to the new, easy to use solution.

6. (Governance NOI Question 2.4.1) Do certain methods of establishing the Steering Group create greater risks to the Guiding Principles?

There does not appear to be a particular threat to how easy solutions are to use that ties directly to Steering Group establishment.

# *APPENDICES*

## APPENDIX A: About OIX

### A.1: Who We Are

The Open Identity Exchange (OIX) is a neutral, technology agnostic, nonprofit enabler of Trust Frameworks for online identity. Its certification credentials can be used across multiple sites, jurisdictions and networks. OIX was founded by a grant from the OpenID Foundation and support from companies including those below.

**OIX Members**

*Executive Members:*
AT&T
Booz Allen Hamilton
CA Technologies
Equifax
Google
PayPal
Symantec
Verizon
Transaction Network Services
LexisNexis

*General Members:*
AOL
ID/DataWeb
Nomura Research Institute
OCLC
Open ID
Pacific East
Prooflink
ProQuest
Sunet
Wave

*Trust Framework Authority Members:*
Connect.Me
Mydex
Kantara Initiative
American Psychological Association

**OIX Board of Directors**

**Kennie Kwong**
AT&T
Lead Member of Technical Staff

Kennie is Lead Member of Technical Staff in the CTO Strategic Standards organization at AT&T, with over 30 years of experience in telecomm and datacomm network and service development, planning and standards. Kennie led the Identity Management Project in the GSM Association featuring global operators and experts from Gemalto (Smartcard) and Microsoft (Information Card), culminating in the publication of the GSMA IdM Framework Document. which investigated the principles of IdM, user privacy, and IdM architecture options leveraging UICC authentication and identity federation to position mobile operators as the IdP.

**Mike Ozburn**
Booz Allen Hamilton
Principal

Mike is currently a Principal at Booz Allen Hamilton. He works within the Information Technology team with a special focus on developing solutions for Civil agencies and Commercial enterprise. Mike is a leader in the Firm's efforts to develop Web 3.0 Trusted Service solutions based on Identity, Trust Management, Data Sharing, and CyberSecurity. He has been active in the development of the emerging Internet trust layer, including the U.S. Government's adoption of Trust Frameworks. In addition to OIX, Mike serves on the boards of the OpenID Foundation, The Information Card Foundation.

**Tim Brown**
CA Technologies
Senior Vice President, Distinguished Engineer, and Chief Architect
Security Management Business Unit

Tim has overall technical direction and oversight responsibilities for the CA security products including Identity Management, Role Modeling and Management, Server Security, Data Loss Protection, Web Access management and Single Sign-on (SSO). With over 20 years of information security expertise, Tim has worked with companies and government agencies implanting security policies and solutions for threat research, vulnerability management, consumer and enterprise identity and access management, network security, encryption and managed security services, and has provided expert witness testimony on these issues before Congress.

**Ron Carpinella**
Equifax
Vice President of Identity Management

Ron is Vice President of Identity Management at Equifax. In this position, he manages the company's initiatives in User Centric Identity Management and has strategic oversight for product development and marketing efforts in this area. Before joining Equifax, Ron served in numerous leadership roles at prominent Internet media and technology companies such as Google, Veoh, Engage Media, Flycast, Fansonly and Relevant Knowledge. Active in many industry organizations, Ron is a member of the Information Card Foundation and the Center for Identity Management Research, among others.

**Eric Sachs**
Google
Product Manager, Security and CIO Departments

Eric has more than 15 years of experience in the areas of user identity and security for hosted Web applications. During his five-plus years at Google, he has worked as a Product Manager for many services, including the Google Account login system, Google Apps for Your Domain, orkut.com social network, Google Health, Google Security, and Internal Systems. Currently Eric works with Google's CIO on an effort to move Google's internal systems to cloud-based technologies by leveraging the same developer tools that Google makes available publicly. In doing so, he is involved with the development of industry standards for data interoperability, including OAuth, OpenID, and OpenSocial.

**Andrew Nash**
PayPal
Senior Director of Identity Services

Andrew is Senior Director in the Information Risk Management and Architecture group at PayPal. Formerly he was CTO at Sonoa Systems and Reactivity working on XML and Service Oriented Architecture processors. As Director of Technologies at RSA Security, Andrew worked on a wide range of identity systems and worked with the Liberty Alliance in the Strong Authentication Expert Group. He is a known leader in PKI and Web-Services security markets, has co-authored numerous Web Services security specifications and is author of a book on Public Key Infrastructure.

**Nico Popp**
Symantec
Vice President, Identity and Authentication Services

Nico heads product development for VeriSign Trust Seal Services, now a Symantec business. Prior to this, Nico was Vice President of Product for VeriSign Authentication Services. In that function, Nico was product manager for the Managed PKI and strong authentication product lines. During his 7 years at VeriSign, Nico has introduced products including VeriSign Identity Protection (VIP), VeriSign Fraud Detection Service (FDS), the Personal Identity Portal (PIP) and VeriSign Trust Seal. Prior to VeriSign, Nico was CTO for RealNames Corp. from 1997 to 2002. Nico was also co-inventor and engineering manager for WebObjects at NeXT Software and Apple Computer.

**Paul Florack**
Transaction Network Services, Inc
Vice President -TSD Product Management

Paul has been part of TNS' Telecommunications Services Division product team since 1993 and is now Vice President responsible for product strategy and business development. Previously, Paul led the company's product management team, which involved overseeing key product launches, including the company's highly successful Calling Identity service and launching of one of the industry's first Inter-Carrier Short Messaging Services.

**Peter Tippett, Ph.D., M.D.**
Verizon Business
Vice President Security Solutions and Enterprise Innovation

Peter is responsible for driving the overall strategic direction of Verizon's industry-leading portfolio of security solutions. Peter has led the computer security industry for more than 20 years, initially as a vendor of security products, and over the past 16 years, as a key strategist. He is credited with creating the first commercial anti-virus product that later became Norton AntiVirus. Peter is known for his creation of enterprise IT metrics, and large risk intelligence and compliance management programs. Peter served on the President's Information Technology Advisory Committee (2003-2005) to guide U.S. efforts in health care IT, information security and computational sciences research. InfoWorld recognized Peter as one of the 25 most influential chief technology officers for 2002.

**Don Thibeau**
OIX Chairman and At-large Director

Don is the Executive Director of The OpenID Foundation (http://openid.nell) an open community software identity standards organization representing leaders in Internet, enterprise and social media technology. He joined the foundation at the beginning of 2009 to represent the organization worldwide and position it for long-term growth. Don has a rich background in the data, identity, and social layers of both the internet and the mobile computing channel. He has both enterprise experience and entrepreneurial management expertise in business models for data, analytics and web content. Don has held senior management positions with leading organizations including Kodak, TransUnion, and LexisNexis. He was an original member of the Reed Elsevier Venture Fund.

Don is a frequent guest speaker and has testified before Congress on topics including data privacy and regulatory issues. He is a member and contributor to e-citizen.org, OASIS, a Booz Allen Distinguished Speaker, a former Presidential appointee and author of numerous articles.

**Nat Sakimura**
At-large Director

Nat is the research lead on Digital Identity at Nomura Research Institute (NRI). He was a co-author of OpenID Provider Authentication Policy Extension (PAPE) specification, the OpenID Connect Core and Artifact Binding specification, JSON Web Token (JWT) specification, XRD specification, and the co-chair of the OASIS Open Reputation Management Systems TC. He has been the elected member of the OpenID Foundation board since 2008 as well as the founding board member of the Kantara Initiative. He has served in various Japanese government committees and is currently a member of the (Identity) Information Coordination Platform Technical Working Group in the Cabinet Secretariat that deals with the forthcoming Citizen Identity system.

**OIX Advisory Board**

**Joni Brennan**
Kantara Initiative
Executive Director

Joni Brennan is the Executive Director of Kantara Initiative. Before this role she was also the Director of Operations and Technology at Kantara Initiative and Liberty Alliance. Joni is one of many players working to move Identity Standards forward though community efforts. Joni's expertise is in Standards Development and Collaborative Virtual Organizations with specific focus on Identity and Security.

**John Henry Clippinger, Ph.D.**
The Law Lab at Harvard University
Founder and Co-Director

John is founder and Co-Director of The Law Lab (www.lawlab.org) at Harvard University, a new multi-disciplinary center founded to research the role of social, neurological, and economic mechanisms on the role of law in facilitating cooperation and entrepreneurial innovation. The Law Lab is developing an open governance platform to enable innovation in governance mechanism to further new forms of private law, self-governance and the formation of digital institutions. John was also a Senior Fellow at the Berkman Center where he helped found and support the development of an open source, interoperability identity framework called Project Higgins (www.eclipse.org/higgins) to give people control over their personal information. He is the author of *A Crowd of One: The Future of Individual Identity* (Perseus, Public Affairs, 2007), and *The Biology of Business, Natural Laws of Enterprise* (Josey Bass, 1998). Previously, he was Director of Intellectual Capital, Coopers & Lybrand and the founder and CEO of four software companies, most recently, Azigo. He consults with companies, foundations, and government agencies on technology, policy and business strategy. John is a graduate of Yale University and holds a MA. and Ph.D. from the University of Pennsylvania. He frequently participates at The Highlands Forum, The Aspen Institute, the CEO Leadership Institute of Yale School of Management, Creative Leadership Summit, Aspen Institute Italy, Fortune Brainstorm, Arab Thought Leadership Conference, Kauffman Summer Institute, Monaco Media Forum, the World Economic Forum Telco Leadership Council, Diamond Exchange, TII/Vanguard, and The Santa Fe Institute Business Network.

**Scott L. David**
K&L Gates, LLP
Partner

Scott is a partner in the K&L Gates LLP law firm. His practice focuses on transaction structuring and providing legal advice associated with emerging technologies including information/data law, compliance with privacy, data security and identity law, electronic commerce, online payment structures, standards setting and tax and intellectual property issues. Scott provides advice to firm

clients on issues of compliance with federal and state privacy and data security laws; structuring of online contracts, terms of use, privacy policies and electronic payment and tax administration systems; networked data risk and liability management; online and telecommunications entity organization and affiliation structuring; technology development and transfer; participation in technical standards setting organizations; international, federal, state and local internet and telecommunications taxation; intellectual property licensing and structuring and non-profit and tax-exempt status and related issues. Scott's publications include chapters relating to telecommunications law and tax issues associated with e-commerce.

In addition, he has authored articles in a variety of journals and publications relating to business information system structuring; legal perspectives on business data security management issues; FCC, FTC and other government regulation of online data and information systems; estate planning in the digital age; payment and tax structuring for online transactions; and broadband over power line (BPL) legal issues. Scott has given presentations on legal issues to a variety of business, legal, and other groups relating to various topics in information law, identity, privacy and data security; monetization and risk mitigation legal strategies for data collection and aggregation; legal issues of commercial interactions using virtual reality interfaces; emerging legal issues in virtual property; issues associated with cloud data storage and services; telecom tax; digital estate planning; nanotechnology; robotics; legal structuring and strategies for technical standards initiatives; and, gift card and stored value card systems. Prior to joining K&L Gates, Scott practiced with Simpson Thacher & Bartlett in New York City. Before attending law school, he worked as the production manager for a computer manufacturer in Rhode Island. Scott is a member of the bars of New York and Washington. He received an LL.M., (taxation) from New York University in 1990, a J.D., from Georgetown University Law Center, 1985 (magna cum laude) and did his undergraduate work at Brown University.

**David Johnson**
Institute for Information Law and Policy, New York Law School
Visiting Professor

David is a graduate of Yale College (BA 1967) and Yale Law School (J.D. 1972). In addition, he completed a year of post-graduate study at University College, Oxford (1968). Following graduation from law school, he clerked a year for Judge Malcolm R. Wilkey of the United States Court of Appeals for the District of Columbia Circuit. David joined Wilmer, Cutler & Pickering in 1973 and became a partner in 1980. David retired as a partner of WCP in 2001. He is currently serving as Visiting Professor at New York Law School, where he is a member of the Institute for Information Law and Policy. (See http://dotank.nyls.edu) His previous legal practice focused primarily on the emerging area of electronic commerce, including counseling on issues relating to privacy, domain names and Internet governance issues, jurisdiction, copyright, taxation, electronic contracting, encryption, defamation, privacy, ISP liability, and intellectual property. David served as founding director of the Aspen Institute Internet Policy Project and as founding president, CEO, and chairman of Counsel Connect, an online meeting place for the legal profession. David has served on the boards of directors of the National Center for Automated Information Research and the Center for Computer Assisted Legal Instruction. He is a co founder of the Law Practice Technology Roundtable. He spent last year as a Senior Resident Fellow at the Center for Democracy and Technology. He now serves on the Advisory Board of Legal OnRamp.

**Thomas J. Smedinghoff**
American Bar Association (ABA) Identity Management Legal Task Force
Co-Chair

Thomas is a partner in the Privacy, Data Security, and Information Law Practice at the law firm of Wildman Harrold in Chicago. His practice focuses on the developing field of information law and electronic business activities, with an emphasis on electronic transactions, identity management, data security, privacy, and corporate information governance issues. Thomas has been actively involved in developing e-business, e-signature, data security, and information legal policy both in the U.S. and globally. He currently serves as co-chair of the Identity Management Legal Task Force of the American Bar Association (ABA) Section of Business Law, and chair of the International Policy Committee of the ABA Section of Science & Technology Law.

Previously, he was chair of the ABA Section of Science & Technology Law (1999-2000) and chair of the ABA Electronic Commerce Division (1995-2003). He is also a member of the U.S. Delegation to the United Nations Commission on International Trade Law (UNCITRAL), where he participates in the Working Group on Electronic Commerce and helped to negotiate the international e-commerce treaty titled the *United Nations Convention on the Use of Electronic Communications in International Contracts and the UNCITRAL Model Law on Electronic Signatures*. He is also the ABA Advisor to the Uniform Law Commission Committee to Implement the UN E-Commerce Convention (2008 -2010), and served as an ABA Advisor to the Uniform Law Commission committee that drafted the Uniform Electronic Transactions Act. Thomas is also the author of the book titled *Information Security Law: The Emerging Standard For Corporate Compliance*, (IT Governance Publishing, 2008). He is also the editor and primary author of the e-commerce book titled *Online Law: The Legal Guide To Doing Business On The Internet*, (Addison Wesley, 1996), as well as numerous articles on electronic transactions, privacy, and data security law issues.

**Hal Warren**
OpenID Society
President

Hal has more than 18 years of experience in Internet technology development specializing in social networking tools and web delivery of commercial content. Currently Hal is working to use emerging trusted identity to build stronger peer circles for scientists and to create better semantics in scholarly publishing. Hal also serves as president of the OpenID Society. He graduated with a BA in philosophy from the University of Tennessee.

## A.2 OIX Tools

Two new OIX Tools are examples of existing infrastructure to facilitate the technical and legal standards development of the Identity Ecosystem Framework: The OIX Knowledge Center Wiki, and OIX Meta Data Listing Service. Please find their descriptions below. For a full list of OIX Programs and Tools please visit: http://openidentityexchange.org/ /.

**OIX Knowledge Center Wiki**

The OIX Knowledge Center Wiki is a common forum for the Open Identity industry to come together to discuss, debate and, most importantly, develop consensus solutions for trust-related problems.

We invite all open identity stakeholders to participate and believe it will provide significant value to:

> **Relying Parties**, to express requirements and gauge the reactions of Users and Identity Providers
>
> **Identity Providers**, to watch the aggregated requirements of Relying Parties and the concerns of Users and be able to shape their offerings accordingly
>
> **Individuals and Users**, to participate in discussions about their concerns about the control and use of their data
>
> **Auditors and Assessors**, to access the latest thinking to shape their product and service offerings without performing new research
>
> **Developers**, to see the consensus developing around the requirements of the market and will be able to learn valuable lessons about the products and services they should develop

We see the Knowledge Center Wiki not only as giving a voice to the Open Identity Industry at large, as being a valuable element of existing infrastructure to support the NSTIC Steering Committee's development of the Identity Ecosystem governance structure.

Please read more at: http://openidentityexchange.org/wiki/knowledge-center.

**OIX Meta Data Listing Service**

The OIX Listing Service will be a publicly-accessible online registry of all of OIX listed Trust Frameworks, together with the assessors, identity service providers, relying parties, auditors, and dispute resolution service providers listed at each Level of Assurance (LOA) and Level of Protection (LOP) for each Trust Framework.

The OIX Listing Service will use a simple, standardized architecture to assign globally-unique Uniform Resource Identifiers (URIs) to each Trust Framework OIX serves, as well as to each LOA, LOP, and technical profile defined in that Trust Framework. In addition OIX will assign URIs to each OIX member participating in the Trust Framework.

Standard queries to the OIX Listing Service will then return concise responses about which identity service providers and relying parties have been certified by which assessors for which Trust Frameworks at which LOA/LOP and for which technical profiles. The OIX Listing Service may also provide other configuration or certification metadata for participants in the Trust Frameworks it serves.

The OIX Listing Service is intended to represent a real-time picture of the online trust ecosystem and the open market for identity assurance and protection services. It is an authoritative source (although not necessarily the only authoritative source) of the metadata necessary to verify the certification status of a Trust Framework participant.

Once an organization is a member of OIX, it can apply for as many listings as it desires in any of the following OIX listing categories:

- Trust Framework
- Identity Service Provider
- Relying Party
- Special Assessor
- Assessor
- Auditor
- Dispute Resolution Service Provider

The OIX Listing Service is currently under development by OIX.

Please read more at: http://openidentityexchange.org/listing-service.

## APPENDIX B: Gallery of Diagrams

**Diagram 1 – Identity Ecosystem as Conceived by NSTIC (Diagram from NSTIC p. 26)**

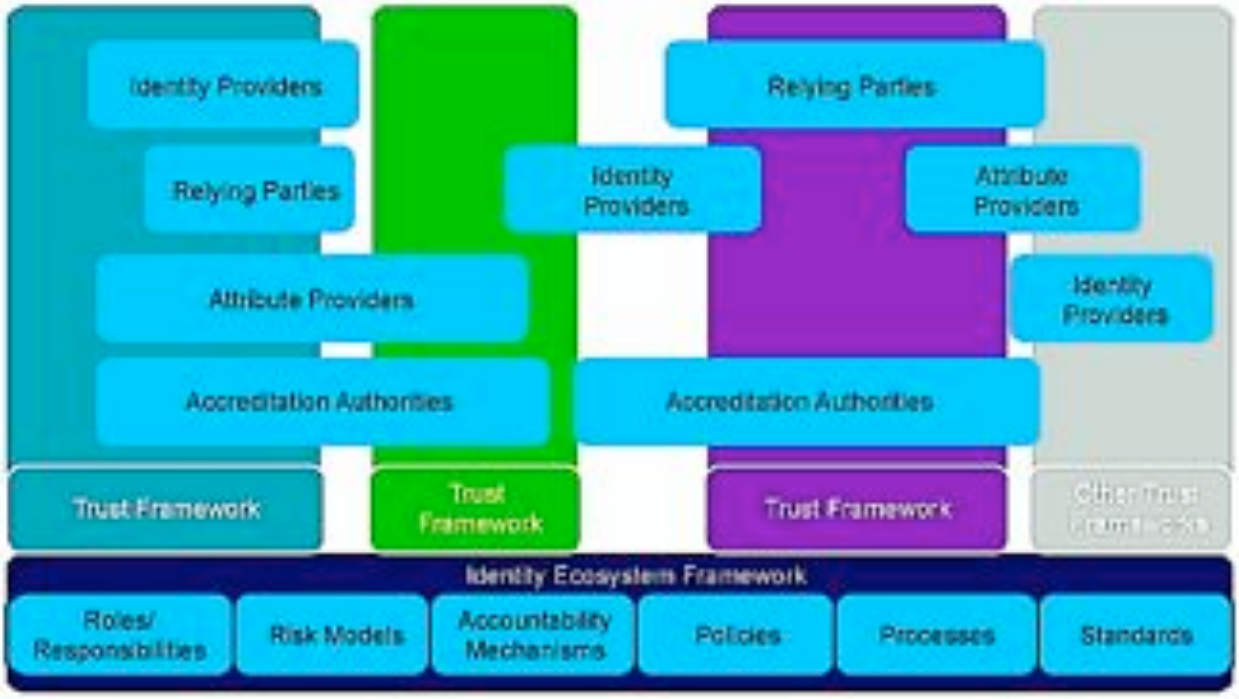


**Diagram 2 – Rulemaking Steps to Building NSTIC Identity Ecosystem**

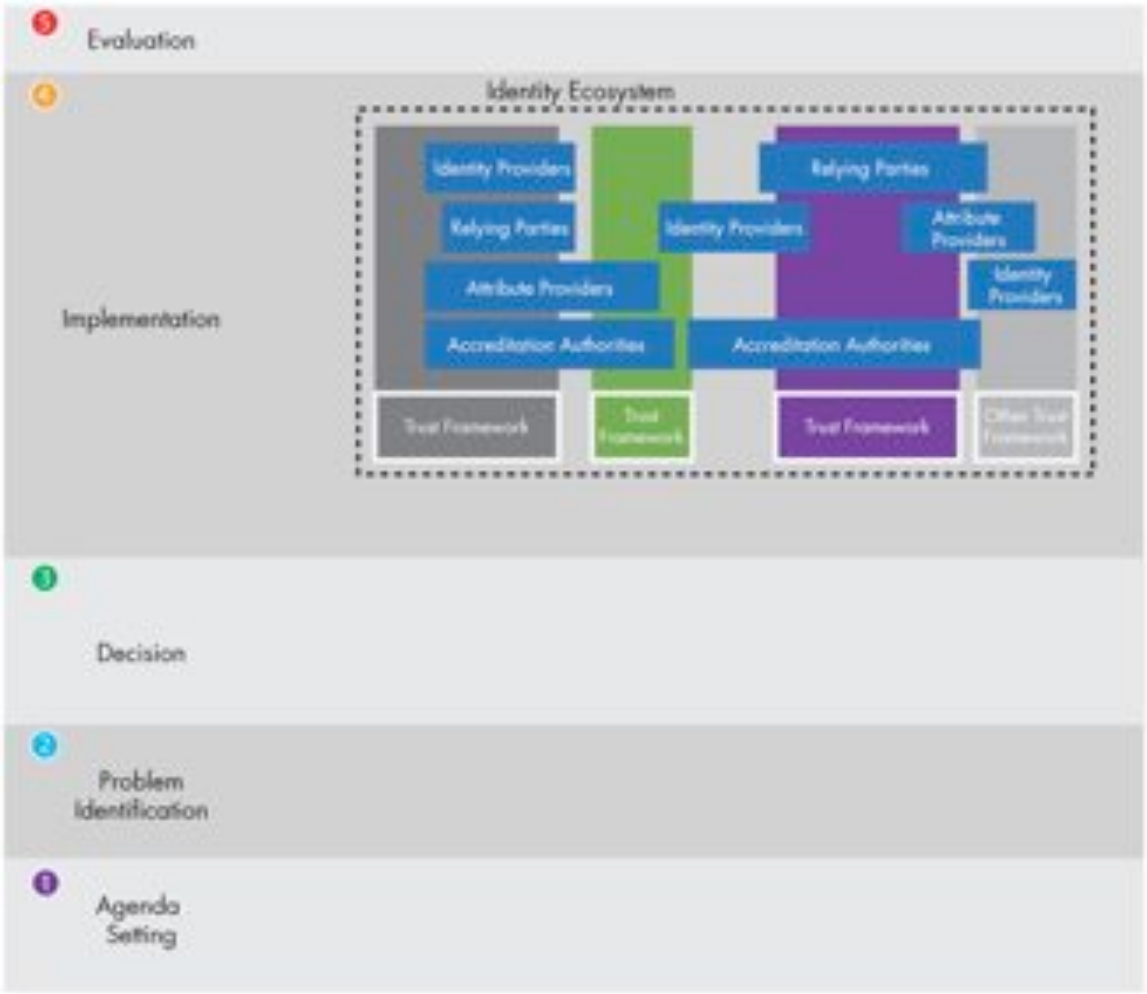


**Diagram 3 – Developing the Trust Framework Components of an Identity Ecosystem**

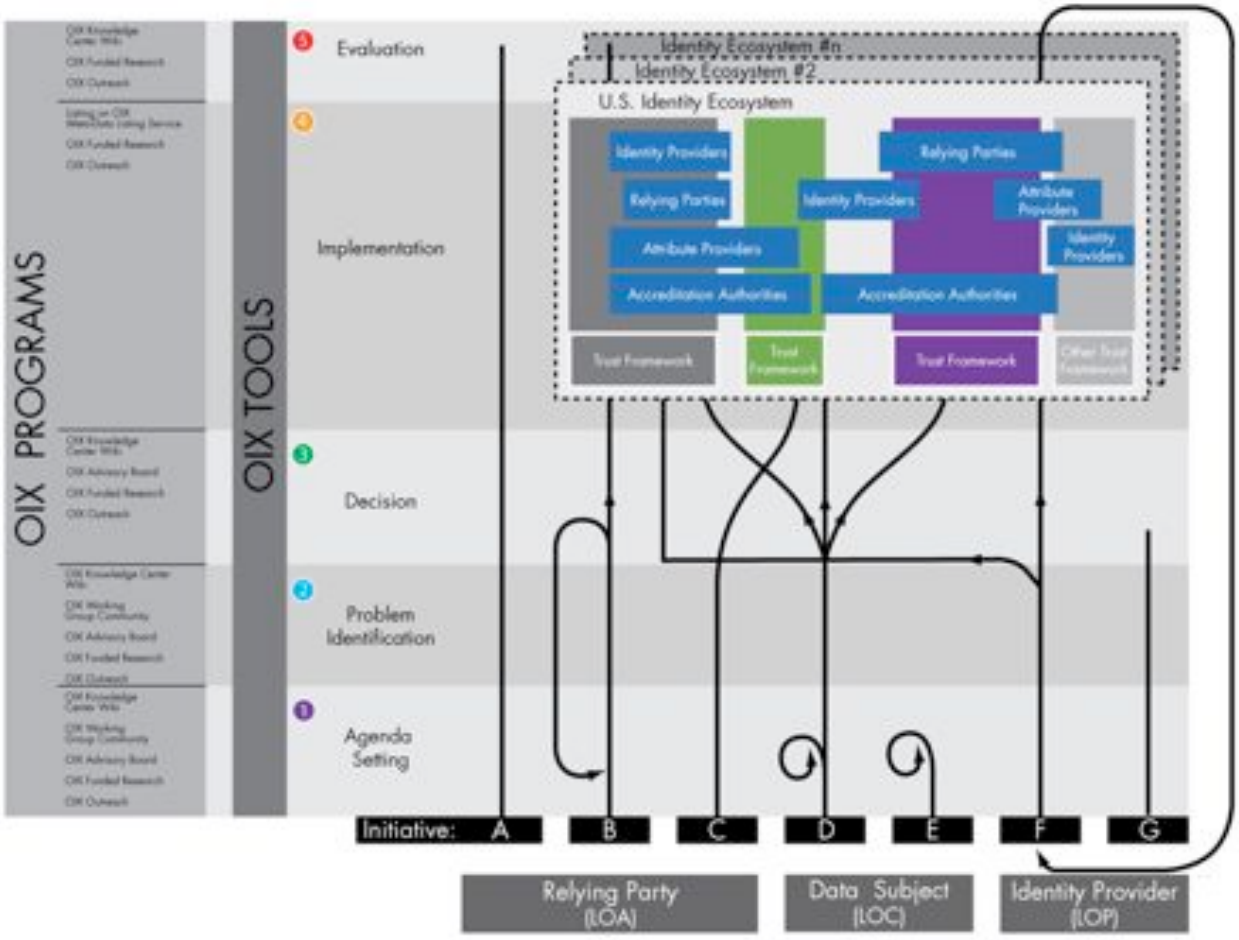


**Diagram 4- Smart Grid: A Potential Model for Steering Group Governance**

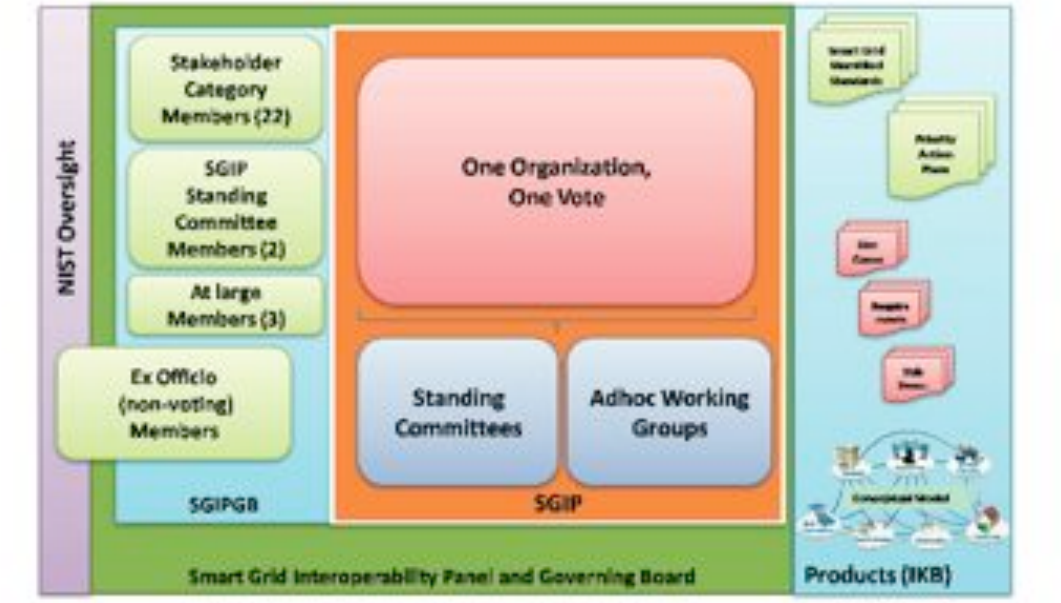


**Diagram 5 - Pathways to Stakeholder Participation**

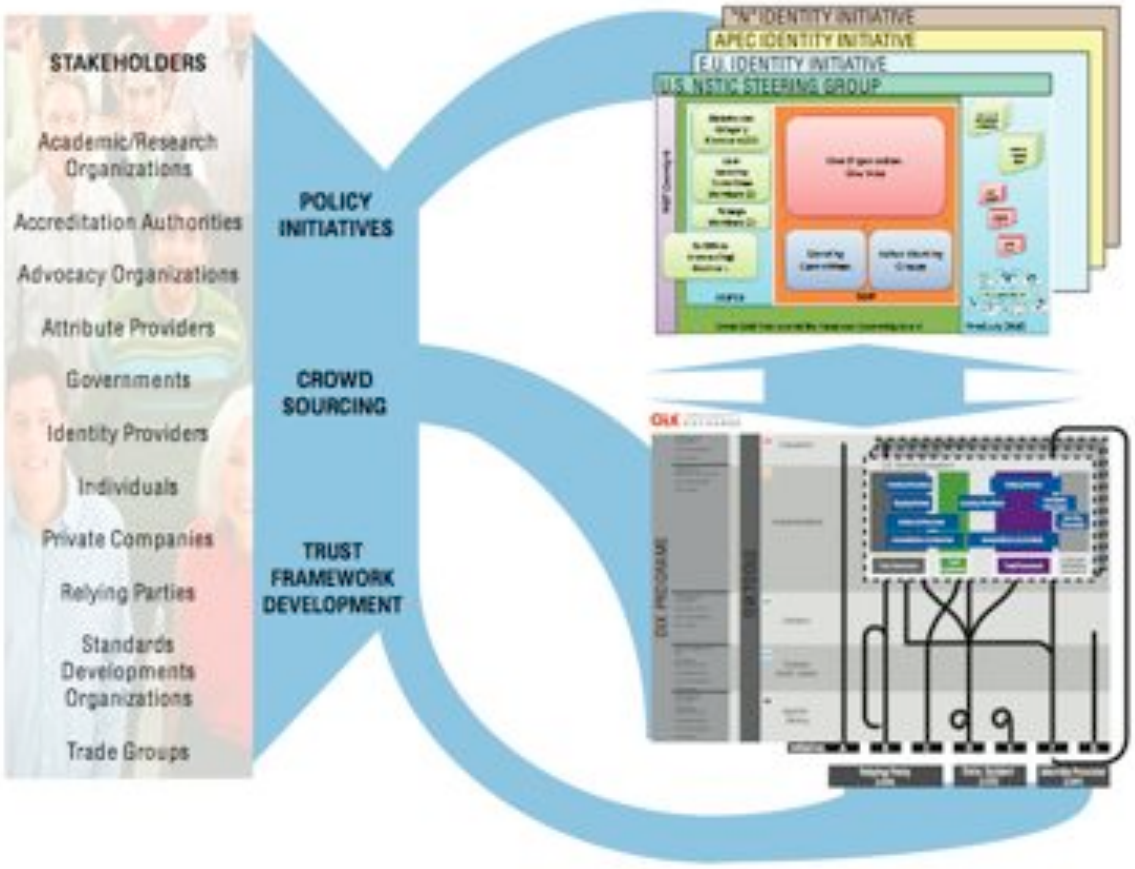


**Diagram 6 - Steering Group Initiation**

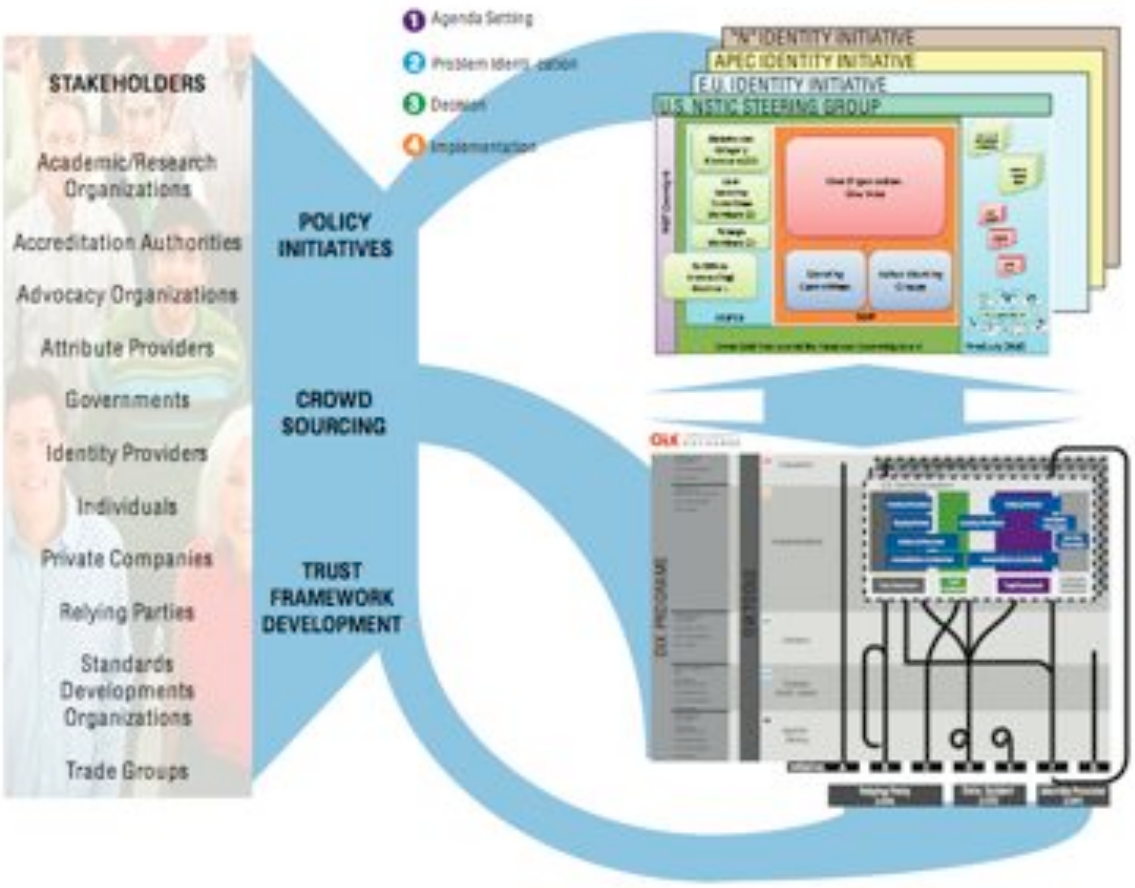


**Diagram 7 - U.S. Steering Group Participation in the Identity Ecosystem**

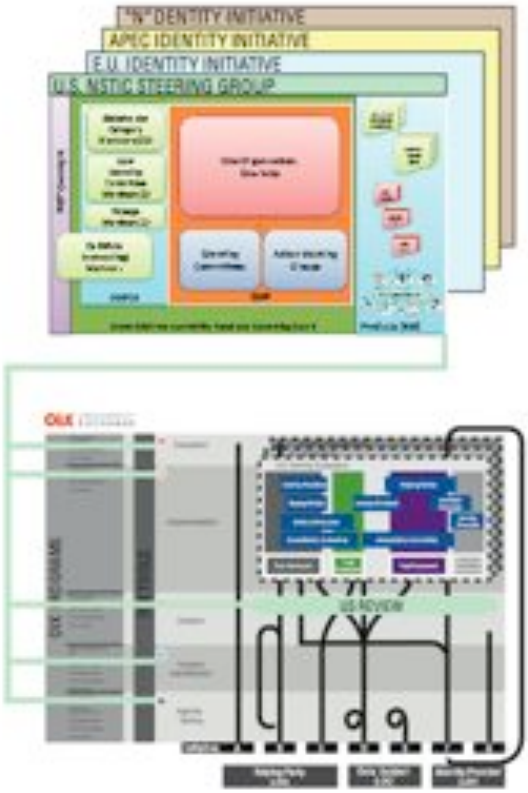
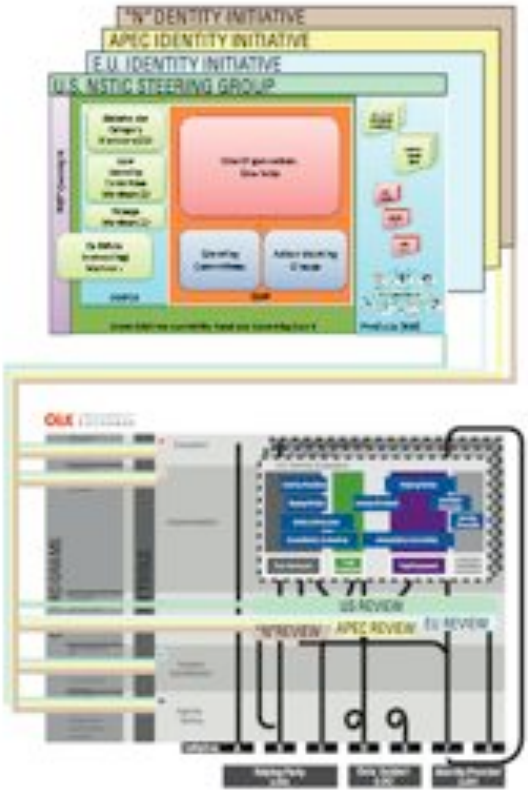


**Diagram 8 - International Initiatives Participation in the Identity Ecosystem**



## APPENDIX C: Proposed Straw Man Draft Charter for Steering Group

Please note that, as discussed in the text, this charter has been prepared based on the Smart Grid Charter (the SGIP and SGIPGB charter). That document was, itself based on the several documents referenced in the charter themselves representing the organizational work of several different associations.

The intention of using these precedents as a starting point is to gain the benefit of the hard work performed by the many people involved in each of those initiatives in working through the issues of how to govern broadly similar settings where broadly networked technologies with multiple stakeholder categories and dimensions needed to work out collective "rules of the road" in order to order their affairs and to normalize their interrelated relationships. No two situations are identical, and the current effort directed at networked data, information, identity systems is certainly going to present a unique set of challenges. Those differences do not, however, preclude the possibility of discerning valuable lessons and replicable governance formalities and structures to inform and assist in the current effort. That is the intention of presenting this draft. It should be thought of as a sort of governance "checklist" of possible governance practice elements, presented in the form of a straw man charter. Some or all of it can be accepted, modified, or rejected as needed.

# UNITED STATES

# NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

# ~~SGIPGB AND SGIP~~ IDENTITY ECOSYSTEM STEERING COMMITTEE

# PLENARY AND GOVERNING BOARD CHARTER

This preliminary discussion draft has been prepared by OIX

as ~~Prepared for~~ a discussion draft, based on the~~:~~

SGIPGB and SGIP Charter

that was prepared for the

**National Institute of Standards and Technology**
100 Bureau Drive Stop 1070
Gaithersburg, MD 20899-1070
USA

~~Prepared~~ by:

**EnerNex Corporation**
620 Mabry Hood Road
Knoxville, TN 37932
USA
(865) 218-4600
www.enernex.com

## TABLE OF CONTENTS

## Executive Summary

Pursuant to the National Strategy for Trusted Identities in Cyberspace, which was signed by President Obama on April 15, 2011 ("NSTIC")~~Energy and Independence and Security Act (EISA) of 2007 [2]~~, the National Institute of Standards and Technology ("NIST"), as part of the Department of Commerce, which has been designated with responsibility to coordinate the U.S. Government's internal National Program Office (the "NPO") for NSTIC, [NOTE: Confirm characterization and trace precise wording of delegation of authority and responsibility through the NOI here] is responsible for helping to initiate the formation of a separate body that will be organized and operated by private parties, which is referred to in the NSTIC as the "Steering Committee."

The Steering Committee will engage in and enable Identity Ecosystem stakeholder "self regulation" and will be responsible, in coordination with the NPO, for ~~coordinating the~~ the development ~~of~~ and publishing of a set of hybrid technical, legal and policy standards for data/identity systems referred to as an "Identity Ecosystem F~~f~~ramework," including protocols and processes and model standards, roles/responsibilities, risk models, accountability mechanisms, and policies to achieve interoperability of Identity ~~Smart Grid devices and~~ Ecosystem technology, legal and policy sub-systems, all with input and cooperation from ~~other Federal and State agencies and~~ interested stakeholders in the social, commercial and governmental sectors~~private sector entities~~. Through the "Participation Governance Model," privately created and promoted Trust Frameworks can voluntarily seek to be reviewed and/or certified for conformance to the Steering Committee's Identity Ecosystem Framework, the intention being that the Identity Ecosystem Framework will act as a hybrid technology tools and legal rules "standard." Conformity by private Trust Frameworks with that standard can help drive interoperability, and foster greater reliability, security, privacy and liability mitigation across networked information systems. The NSTIC anticipates that the Steering Committee will develop the standard to which its members will then be subject.

This Charter sets forth the basic structure of organization and operation of that Steering Committee. In recognition of the need to address networked information system issues at both I~~i~~nternet and local scale, the structure of the Steering Committee is intended to foster participation. Toward this end, it has a two part structure composed of an open Steering Committee "plenary" body, and a governance board the membership of which is elected directly by the members of the Plenary. It is intended that the "standards" that emerge from the Steering Committee reflect the balanced needs of the many stakeholders in online data/identity systems, which is intended to be reflected in the composition of the Steering Committee plenary. The Steering Committee Governance Board is intended to help organize the plenary, and to operate the Steering Committee in a manner that maximizes its ability to solicit and reflect the data/identity system needs of all the stakeholders represented by the plenary.

The Identity Ecosystem ~~Smart Grid~~ Interoperability P~~l~~enary~~anel~~ (IE~~SG~~IP) is a membership-based organization formed as a ~~created by an Administrator under a contract from NIST~~ [NOTE: This section can be completed at such time as the form of organization and the manner of its organization and operation are more clearly defined. Also consider whether the Steering Committee should seek recognition of exemption under Internal Revenue Code section 501(c)(3)(consider purposes including "educational" or "lessening the

burdens of government"), 501(c)(6) (trade association) or another section; also consider other potential organizational and status issues to permit maximum flexibility to accommodate stakeholder needs] to provide an open process for stakeholders to participate in providing input and cooperating with one another~~NIST~~ in the ongoing coordination, acceleration and harmonization of technical standards and legal/policy standards development ("Tools and Rules") for the Identity Ecosystem~~Smart Grid~~. The ~~SG~~IEIP, through its various committees and working groups, also reviews use cases, identifies requirements and architectural reference models, coordinates and accelerates Identity Ecosystem~~Smart Grid~~ testing and certification, and proposes action plans for achieving these goals [NOTE: modify and add to list of activities once defined]. The ~~SGIP~~IEIP will not initially ~~does not~~ write ~~standards~~Trust Framework standards for the Identity Ecosystem, but serves as a forum to coordinate the development of standards and specifications by many standards development organizations. Once it has had the opportunity to work with existing Trust Framework standards sufficiently to discern "best practices," it may begin to develop a set of independent Identity Ecosystem Trust Framework standards to address stakeholder needs in comprehensive and/or more focused way [NOTE: Confirm whether the foregoing is accurate.].

The ~~SGIP~~IEIP will itself be managed and guided by a Governing Board that approves work programs for the ~~SGIP~~IEIP to carry out its work efficiently and effectively, prioritizes work, and arranges for the necessary resources. The Governing Board's responsibilities include facilitating a dialogue with standards development organizations to ensure that the action plans can be implemented. When the IEIP engages in the activity of generating independent Identity Ecosystem Framework standards, the IEIPGB will help coordinate those standards to foster reliability and interoperability across sectors and to balance the interests of multiple stakeholder groups affected by such standards. [NOTE: Consider other activities that will be engaged in by the governing board].

## A note regarding the form of IEIP and IEIPGB charter

This Charter for the IEIP and the IEIPGB is based on the Charter for the Smart Grid Interoperability Panel and the Smart Grid Interoperability Panel Governing Board. That charter, in turn, indicates that~~T~~ the structure and organization of the SGIP and SGIP Governing Board (SGIPGB) were based substantially on the design of two principal existing organization structures:

The Healthcare Information Technology Standards Panel (HITSP) [8], which is similar in nature to the SGIP, and,

The GridWise® Architecture Council (GWAC) [3][4], which is similar in nature to the SGIPGB.

The SGIP Charter also indicates that t~~T~~he contents of its charter~~this~~ document were substantially influenced by the structure of the following organizations:

American National Standards Institute (ANSI) [1]

Internet Engineering Task Force (IETF) Internet Architecture Board (IAB) [7]

Utility Communication Architecture International users' group (UCAIug) [9][10]

## IEIP Committees and Working Groups

It is envisioned that the ~~SGIP~~IEIP will have at least two permanent committees. One permanent committee will be responsible for [NOTE: Review and modify the following as necessary] creating and refining an architectural reference model, including recommended ~~standards~~Trust Framework standards and profiles necessary to implement the vision of the ~~Smart Grid~~Identity Ecosystem. The other permanent committee will create and maintain the necessary documentation and organizational framework for testing conformance with these ~~Smart Grid~~Identity Ecosystem ~~standards~~Trust Framework standards and specifications. The ~~SGIP~~IEIP, as needed, may form additional permanent committees and ad-hoc working groups.

## Public Access and Involvement through the Participation Governance Model

Unlike the SmartGrid Model, the IEIP and IEIPGB have access to substantial existing resources to help with their work. These resources include the advanced Trust Framework technical development work of numerous standards setting organizations and the Trust Framework development and market support programs and tools of the Open Identity Exchange, a not-for-profit organization formed to improve the conditions in the data/identity sector generally.

[NOTE: Insert paragraph summarizing how the IEIP can benefit from existing standards organizations work and structure. Outside of Steering Committee charter creation, consider compiling "resource list" detailing liaison, resource sharing, and other coordination opportunities with specific existing programs.]

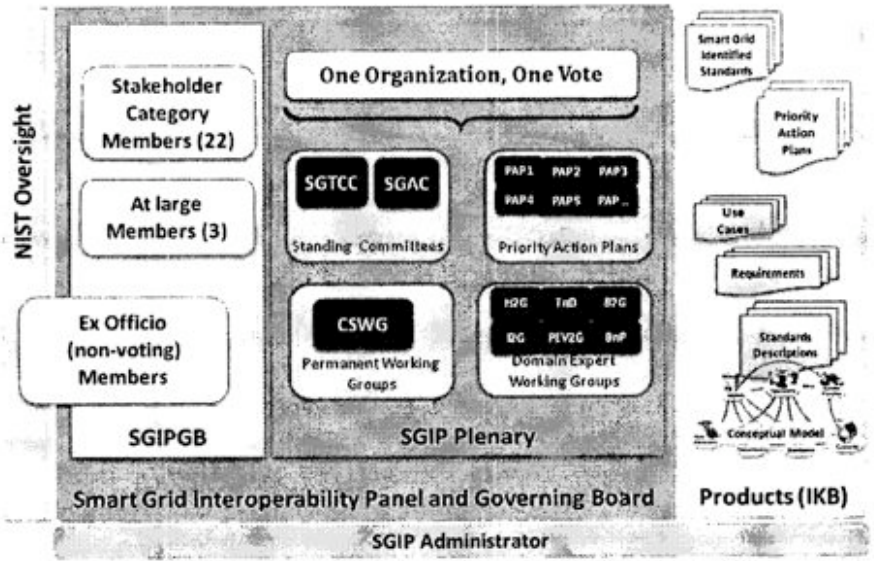
[NOTE: Consider whether IEIP public outreach programs could benefit from use of OIX programs and tools] All ~~SGIP~~IEIP outputs will be delivered to the public through the OIX~~NIST Smart Grid~~ Knowledge Center ~~Collaborative~~ Wiki and the online [OIX?][IEIP?][Interoperability Knowledge Base (IKB)] website. [NOTE: The following FACA reference should be reviewed against the statute. Also, consideration should be given to the potential treatment of Steering Committee charter proposals under FACA]The Federal Advisory Committee Act prohibits [NIST][NIST or the NPO] from accepting advice directly from the ~~SGIP~~IEIP. The development work has been structured so that no advice is provided to NIST. Instead, [NOTE: Insert description of arrangements here]. ~~Therefore NIST has contracted with the Administrator to provide advice to NIST by refining SGIP outputs using their technical expertise including but not limited to analyzing, identifying gaps, and making their own recommendations), prior to providing them to NIST.~~

## IEIP Composition and Organization

The ~~SGIP~~IEIP and its governing board (together referred to as the "Steering Committee") is~~are~~ an open organization dedicated to balancing the needs of a variety of ~~Smart Grid~~Identity Ecosystem-~~-~~related organizations. Any organization may become a member of the ~~SGIP~~IEIP. Members will be required to declare an affiliation with a single, ~~a~~ identified Stakeholder Category (_____ ~~twenty-two~~ have thus far been identified ~~by NIST~~ and are listed in Appendix A). Members may contribute multiple Member Representatives, but only one Voting Member Representative. Participating Members must participate regularly in order to vote on the work products of the panel.

It is envisioned that the ~~SGIPGB~~IEIPGB will include at least one Member from each Stakeholder Category, the chairs of two permanent committees, several "members at large", and several ex officio members representing for example, key government agencies. New ~~SGIPGB~~IEIPGB members will be recommended by a candidate evaluation committee and approved by the ~~SGIPGB~~IEIPGB as a whole. Terms of ~~SGIPGB~~IEIPGB members will be staggered to ensure both regular turnover and continuity.

The diagram (see below) represents the relationships between the concepts proposed in this draft charter document. The final charter document will include a final version of this diagram with comments from the public addressed.



*This page intentionally blank*

# 1. Mandate

## *1.1 ~~SGIP~~IEIP Charge and Mission*

### *1.1.1 ~~SGIP~~IEIP Charge*

The ~~Smart Grid~~Identity Ecosystem Interoperability Panel (~~SGIP~~IEIP) is being created ~~through a contract from~~ in cooperation with the NPO that is coordinated out of the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. The government's role in the IEIP is intended to be limited to support and [ ] [NOTE: Include scoping language from NSTIC and NOI here] during the initiation phase. The NSTIC calls for the Steering Committee, of which the IEIP and the IEIPGB are two subparts, to be organized and operated as a privately-led body. This charter starts to establish the details of how that body will be organized and operated, with the intention that the stakeholders themselves will have ultimate control of the focus and activities of the Steering Committee.

[NOTE: Consider whether the following is to "provocative." It is intended to create a common expectation that the Steering Committee focus and auspices is likely to need to evolve as stakeholder needs change in a rapidly maturing data/identity market. Setting this expectation at the inception of the process may help to focus participants on issues and tasks that are more effectively and efficiently organized into logical stages, etc.]. Steering Committee independence is critical to its ability to be responsive to changing technologies and the new and expanded markets that they generate. Accordingly, and in order to be able to accomplish its charge under the NSTIC, the Steering Committee auspices may be expanded (by the affirmative action of the IEIP working through the IEIPGB) beyond those contemplated by NSTIC, but its activities, will continue to be consistent with and supportive of the goals of NSTIC; making explicit the tacit understanding that results from the fact that the NSTIC "call to action" to which the Steering Committee is expected to respond, is a U.S. government document prepared with comment from the private sector, that will likely benefit from continued stakeholder efficacy in agenda setting and the discretion to identify stakeholder-critical needs. NSTIC is a starting point, and the government will continue to play a critical monitoring and other supporting role, but a sustainable, inclusive, transparent, participatory, independent, consensus building, private sector-led Steering Committee structure will ultimately best serve the goals of NSTIC. ~~to support NIST's role as defined in the Energy Independence and Security Act (EISA) of 2007 to "coordinate the development of a framework that includes~~

~~protocols and model standards for information management to achieve interoperability of smart grid devices and systems."~~[NOTE: Insert NSTIC reference to Steering Committee here] The ~~SGIP~~IEIP will provide an open process for Stakeholders to participate in providing input and cooperating with the IEIP~~NIST~~ in the ongoing coordination, revision, acceleration and harmonization of ~~standards~~Trust Framework standards development for the ~~Smart Grid~~Identity Ecosystem. The ~~SGIP~~IEIP members participate in an open process to [NOTE: Review and revise the following as appropriate]:

provide technical and business guidance resulting in use cases, requirements, and recommended Trust Framework standards:

recommend revisions to existing ~~standards~~Trust Framework standards; identify gaps in existing ~~standards~~Trust Framework standards:

coordinate ~~Smart Grid~~Identity Ecosystem testing and certification programs: and

recommend Priority Action Plans (PAPs) for accelerating the ~~standards~~Trust Framework standards development and testing and certification of components for the ~~Smart Grid~~Identity Ecosystem.

### *1.1.2 ~~SGIP~~IEIP Mission*

The mission of the ~~SGIP~~IEIP is to provide a strong framework for coordination of all stakeholders of the ~~Smart Grid~~Identity Ecosystem to accelerate ~~standards~~Trust Framework standards harmonization and development. In its initial phases, t~~T~~he ~~SGIP~~IEIP will not ~~does not~~ write ~~standards~~Identity Ecosystem Framework standards, but instead will develop~~s~~ and review~~s~~ use cases, identif~~y~~~~ies~~ requirements, and propose~~s~~ action plans for achieving these goals. [NOTE: Consider issues of relationship of Trust Framework standards developed in individual Trust Framework initiatives and the overall "top of the US stack" Identity Ecosystem Framework contemplated by the NSTIC. The activity of the Steering Committee (composed of the IEIP and the IEIPGB) could be to write independent standards, or to identify market-based "best practices" for promotion as standards, or some combination thereof. This draft is directed at the initial "doing homework" period where the Steering Committee will need to study stakeholder needs and identify available technology and Trust Framework options prior to drafting or adopt standards for application at the Ecosystem Framework level. During this period, it is assumed that there will be a delay in creating Ecosystem Framework level standards while that review takes place. Thereafter, the Plenary and the Governing Board can work together to expand their collective mission to include the creation of new standards as necessary to compliment the available options in the market, toward the Identity Ecosystem Framework standards goals set forth in NSTIC. The proper structure of those standards should be informed by and balance all stakeholder needs. As a result, it may, at present, be premature to attempt to structure the process through which those standards would be derived from group consensus processes of the IEIP at the initial stages before the needs are understood]

The ~~SGIP~~IEIP has three principal responsibilities:

a. To provide the technical guidance necessary to facilitate ~~standards~~Ecosystem Framework standards development for the ~~Smart Grid~~Identity Ecosystem

b. To specify the necessary testing and certification requirements to assess the achievement of interoperability using ~~Smart Grid~~Identity Ecosystem ~~Standards~~ Framework standards

c. To oversee the performance of these activities to maintain momentum and achievement

d. [List other purposes here]

### *1.2 ~~SGIP~~IEIP Scope*

#### *1.2.1 ~~Smart Grid~~Identity Ecosystem ~~Standards~~Trust Framework standards*

The ~~SGIP~~IEIP will provide a forum for discussion and coordination among organizations that write and publish ~~standards~~Trust Framework standards documents and for those parties that are stakeholders in those Trust Frameworks. Those Trust Framework standards will generally be recorded and presented in the form of written Trust Frameworks, or subparts thereof. The ~~SGIP~~IEIP recommends documents indicating selections and profiles of Trust Framework standards developed by other organizations that are appropriate for use in the ~~Smart Grid~~Identity Ecosystem. These ~~standards~~Trust Framework standards, developed and published by standards development organizations, may be pre-existing, in development, or in need of a new standards development effort. They may be proprietary, open standards, or some combination thereof, provided that if and when the IEIP adopts proprietary Trust Framework standards as part of its Ecosystem Framework standards, it will follow the disclosure and marking practices set forth in Exhibit 1.2.1A

~~Standards~~Trust Framework standards that are identified for inclusion by normative or informative cross reference to all or part thereof ~~use~~ in the ~~Smart Grid~~Identity Ecosystem Framework and the ~~standards~~Trust Framework standards development process to produce them remain the purview of the SDOs developing them.

#### *1.2.2 Priority Action Plans*

The ~~SGIP~~IEIP maintains Priority Action Plan documents, recommended ~~standards~~Trust Framework standards lists, and the ~~smart grid~~Identity Ecosystem conceptual model and its derivatives. The ~~SGIP~~IEIP will from time to time publish written definitions and clarifications of its recommendations in support of its mission.

#### *1.2.3 Testing and Certification of ~~Standards~~Trust Framework standards*

A key activity of this organization is to develop, foster, and implement clear certification criteria by which ~~standards~~Ecosystem Framework standards of the ~~Smart Grid~~Identity Ecosystem, as recognized by this body, can be verified through testing of products and services offered by vendors. It is recognized that in the early stages, the IEIP and the IEIPGB will focus on discernment of market "best practices" and other criteria to identify candidates for consideration as Identity Ecosystem Trust Framework standards.

#### *1.2.4 ~~Smart Grid~~Identity Ecosystem Conceptual Model*

The ~~SGIP~~IEIP maintains and extends the utility and content of the ~~Smart Grid~~Identity Ecosystem Conceptual Model introduced in the NSTIC vision of the Identity Ecosystem~~NIST~~ Framework.

#### *1.2.5 ~~Smart Grid~~Identity Ecosystem Cyber Security, Privacy and Online Identity Integrity*

The ~~SGIP~~IEIP conducts analysis and studies on the requirements of ~~standards~~Trust Framework standards to support cyber security, privacy and online identity integrity for the ~~Smart~~

~~Grid~~Identity Ecosystem. Therefore the ~~SGIP~~IEIP will provide a forum for the discussion of an evolution of the knowledge and plans on this critical subject.

### *1.2.6 The OIX Online ~~Interoperability~~ Knowledge Center~~Base~~ (OOKC~~IKB~~)*

In an effort to leverage existing resources, save costs and integrate Steering Committee operations with existing sources of relevant data/identity market ~~The~~information, the ~~SGIP~~IEIP may distribute~~s~~ the results of its efforts through the OIX Online ~~Interoperability~~ Knowledge Center ~~Base~~ (OOKC~~IKB~~). This resource, which is integrated with related ~~national~~ web-based resources, provides ready access for both technical and non-technical stakeholders of the ~~Smart Grid~~Identity Ecosystem to the information content generated by the ~~SGIP~~IEIP combined with other market relevant information and development tools and support maintained by OIX and contributed by stakeholders throughout the global identity ecosystem. The ~~SGIP~~IEIP documents will be posted at the OIX~~NIST Smart Grid Collaborative~~ Knowledge Center Wiki Site at _____. A variety of public documents and professional conference presentations and publications are available on this site.

### *1.2.7 Enlisting Stakeholder Involvement*

The ~~SGIP~~IEIP will enlist involvement from a broad selection of ~~Smart Grid~~Identity Ecosystem Stakeholders to:

a. Accelerate ~~standards~~Trust Framework standards-based interoperability across online networked data and identity~~the electric power~~ system~~s~~;

b. Identify and prioritize the concepts, ~~standards~~Trust Framework standards and architectures needed to make interoperability possible, guided by an Architecture Committee;

c. Describe and prioritize clear, practical steps that will facilitate the interoperation of the systems, devices, and institutions that participate in the use and operation of the Identity Ecosystem~~nation's electric system~~; and

d. Assess ~~Smart Grid~~Identity Ecosystem interoperability standards conformity through a structured, open framework of documents and organizations, guided by a Testing and Certification Committee.

### *1.2.8 Out of Scope*

[NOTE: The following should be clarified to anticipate the manner in which the IEIP will work toward producing the Identity Ecosystem framework. It is relevant whether the Trust Framework standards set forth in that document will be "homegrown" or will be constructed from normative cross references to Trust Framework legal, technical, policy and other evolving standards present in the market. Language will be needed to capture these relationships as the path of the Steering Committee activity becomes clearer during the initiation phase. It is possible that the IEIP can demonstrate leadership in the area by following and normalizing market trends.] The ~~SGIP~~IEIP will not initially write or publish ~~standards~~Trust Framework standards documents; it will seek to identify and combine market-based standards that are

consistent with the NSTIC that it will work to shape into an integrated, coherent, flexible and resilient Identity Ecosystem Framework.

The ~~SGIP~~IEIP is not a government organization. It is a private sector~~ublic~~ body created [NOTE: Insert reference to form of organization and manner of operation here]~~under a contract from NIST to an Administrator to support NIST in its role under the EISA 2007 [2]~~. Its publications are not legal documents, laws or regulations. [NOTE: Include elaboration of Trust Framework standards development process here. Include references to potential mechanisms to recognize and formalize industry and community "standards of care." Include references to potential adoption of Steering Committee standards as "codes of conduct" that may be enforced by both private and public mechanisms.].

The ~~SGIP~~IEIP will not design, promote or sell products or technologies suggested by its deliverables.

### *1.3 ~~SGIP~~IEIP Expected Results and Actions*

The ~~SGIP~~IEIP provides a single mechanism with comprehensive and complete ~~Smart Grid~~Identity Ecosystem Stakeholder representation that facilitates consensus-based approval of national ~~Smart Grid~~Identity Ecosystem ~~standards~~Trust Framework standards.

#### *1.3.1 ~~SGIP~~IEIP Activities*

The activities of the ~~SGIP~~IEIP will include, but not necessarily be limited to:

a. Facilitating the timely development and harmonization of ~~standards~~Trust Framework standards responsive to identified interoperability, security, privacy system integrity, and liability and risk limitation issues for all stakeholders, and meeting the requirements of identified use cases;

b. Recommending creation or dissolution of committees;

c. Activating a conflict resolution mechanism, as needed;

d. Performing all other acts necessary and appropriate to the conduct of the ~~SGIP~~IEIP's activities and achievement of the ~~SGIP~~IEIP's Charge;

e. Disseminating the ~~SGIP~~IEIP outputs (through the use of and in coordination with publicly accessible Open Identity Exchange Tools and Programs) and promoting the use of the recommended ~~standards~~Trust Framework standards;

f. Establishing a framework for Testing and Certification of ~~Smart Grid~~Identity Ecosystem Components.

g. Maintenance of the ~~Smart Grid~~Identity Ecosystem Architecture [NOTE: To the extent that Architecture Maintenance can be made more effective and inclusive through application of the Participation Governance Model and through use of OIX tools, consider reference here].

h. [Other?]

### *1.3.2 Publication of Operations*

Essential information about all ~~SGIP~~IEIP activities will be publicly available via the ~~SGIP~~IEIP website and through the OIX Knowledge Center.

### *1.3.3 Use Cases and Requirements*

Domain expertise will be provided by the ~~SGIP~~IEIP via the identification of detailed Use Cases and the analysis of requirements that are necessary to support them. These Use Cases illustrate the context of technical analyses and recommendations that the ~~SGIP~~IEIP relies upon to identify needed priority action plans and recommended ~~standards~~Ecosystem Framework standards.

### *1.3.4 The Interoperability Knowledge Base*

Resulting Use Cases and Requirements, along with analyses and white papers produced by the ~~SGIP~~IEIP, will be integrated into the OIX Online Knowledge Base~~IKB~~ for review and comment by the Stakeholders of the ~~Smart Grid~~Identity Ecosystem. [NOTE: check references to wiki and knowledge base for consistency. The intention is to make clear that the steering committee has access to full use of OIX tools and programs so that it doesn't have to reinvent the wheel when it comes to outreach tools and information gathering tools to perform its work. The OIX tool set, combined with the listing service program, provides direct access to the market for purposes of Steering Committee input and output interactions].

## *1.4 ~~SGIP~~IEIP Principles*

### *1.4.1 Openness*

The work of the ~~SGIP~~IEIP, including all working groups and committees, will be open for public review as follows:

a. All minutes of all meetings will be posted on the Internet.

b. All documents and drafts under discussion will be posted on the Internet.

c. All meetings are open to public attendance.

### *1.4.2 Balance*

The ~~SGIP~~IEIP will be organized on the principle of balancing representation across multiple industry segments related to online data and identity systems~~electric energy~~ and the technology necessary to effectively manage it. The design of the organization will enable it to:

a. Carry out its mission effectively; and

b. Provide leadership throughout the ~~Smart Grid~~Identity Ecosystem Stakeholder community.

### *1.4.3 Consensus*

Consensus is a core value of the ~~SGIP~~IEIP. For purposes of the ~~SGIP~~IEIP, consensus means the general agreement of the Members. The process of the ~~SGIP~~IEIP, including the ~~SGIPGB~~IEIPGB and all working groups and committees, requires the respective Chairs to ensure consideration of all views, proposals and objections, and to endeavor to reconcile them. Where consensus is not possible, the ~~SGIP~~IEIP, including the ~~SGIPGB~~IEIPGB and all working groups and committees, will strive to make decisions that are supported by the available information and to document opposing views or abstentions.

The achievement of consensus will be based on thorough examination of issues, including the discussion of dissenting opinions and the resolution of disagreements. Consensus will be preferred to resolve all issues brought before the ~~SGIP~~IEIP, including the ~~SGIPGB~~IEIPGB and all working groups and committees. For purposes of the ~~SGIP~~IEIP, consensus means a general agreement by all members.

When a disagreement exists, a vote will be taken to reach consensus.

### *1.4.4 Harmonization*

The ~~SGIP~~IEIP process encourages harmonization among ~~standards~~Trust Framework standards. Decisions are relevant and effectively respond to regulatory compliance and market needs, as well as technological developments to achieve essential interoperability, security, privacy and liability and risk limitation characteristics.[NOTE: There are several provisions that make reference to the Smart Grid's goal of "interoperability." Interoperability is also a central goal of the NSTIC in addition to other goals. The NSTIC goals are further expanded by reference to various private parties' interests such as robust authentication, identity integrity, security, privacy, liability limitation and mitigation, cost savings, resiliency, transparency and a host of other considerations. Many of these issues can be best addressed through the legal policy equivalent of the "network effect," i.e., they are best solved when standardized, normalized, common systems are adopted by broad populations of stakeholders. The linchpin to achieving the desirable network effects is broad adoption. The key to broad adoption is to address stakeholder needs. Taken together, the systems that are best able to address stakeholder needs will be those that are most broadly adopted, and the systems that are most broadly adopted will be those that best address stakeholder needs. This tautology reflects the simple reality that the many desirable system characteristics "emerge" from the network effect of broad adoption, and suggests that references to "interoperability" in the charter as a core goal should be expanded to include at least the general categories of stakeholder needs identified to date. One way to deal with this in the charter is to create a defined term (which might be "Interoperability" or another word) to describe the set of stakeholder-desired system characteristics]

For any standard gap, interested SDOs and other stakeholder groups will prepare a justification to present to the ~~SGIP~~IEIP relative to how the standard fits into their organization, and how they will position their work to support interoperability [NOTE: reference to other system goals here? See note above] and integrate with other ~~NIST-identified~~ ~~standards~~Ecosystem Framework standards for the ~~Smart Grid~~Identity Ecosystem. The ~~SGIP~~IEIP, or working group thereof, can then select from these offerings to identify a work project.

#### 1.4.5 Leveraging of Applicable Standards

In general, IEIP should focus on Identity Ecosystem Trust Framework level guidelines or "standards" at the legal, policy and conceptual architectural levels. Should technical standard gaps be identified and protocol level technical standards be required, engagement of appropriate SDO/industry fora (e.g., Kantara, OASIS, IETF, W3C and OIDF) to develop the required technical standards should take precedence over creating new IEIP Working Groups to develop such standards.

In addition, any decision to adopt, endorse or profile a specific Identity or Trust Framework standard solution as part of the Identity Ecosystem Framework must take into account its inherent cost-effectiveness, specifically:

- To ensure that any additional complexity involved is commensurate with the security demands of the relevant usage scenarios; and
- To take into account life-cycle costs of ownership and operations. This latter principle is important to align with increasingly challenging economic conditions, and to ensure sustainability of the ecosystem as a whole.

### 1.5 ~~*Smart Grid*~~*Identity Ecosystem* Interoperability Panel Governing Board (~~*SGIPGB*~~*IEIPGB*)

The ~~SGIP~~IEIP will be managed and guided by a Governing Board that approves and prioritizes work programs and arranges for the resources necessary to carry out finalized priority action plans. The Governing Board's responsibilities include facilitating a dialogue with standards development organizations to ensure that the action plans can be implemented. The ~~SGIPGB~~IEIPGB provides guidance to the ~~SGIP~~IEIP. This guidance includes a broad perspective of the NSTIC~~NIST Interoperability Framework and Roadmap vision~~. The Administrator reports on progress by maintaining the ~~Smart Grid~~Identity Ecosystem Roadmap, [NOTE: consider whether the "Roadmap concept" will be carried forward into Identity Ecosystem Work] and ensures all ~~SGIP~~IEIP documents are openly available through the Open Identity Exchange Online Knowledge Base~~in an online Interoperability Knowledge Base~~.

#### 1.5.1 ~~*Smart Grid*~~*Identity Ecosystem* Interoperability Panel Governing Board Tasks

To execute its mission, the ~~SGIPGB~~IEIPGB will:

a. Guide the ~~SGIP~~IEIP in executing its mission of developing ~~standards~~Trust Framework standards-based interoperability technology and best practices by integrating the needs, ideas and priorities expressed by a broad Stakeholder base;

b. Approve work program for the ~~SGIP~~IEIP, including Priority Action Plans (PAPs).

c. Provide guidance for ~~SGIP~~IEIP to recommend ~~standards~~Trust Framework standards based on ~~SGIP~~IEIP activities.

d. Ensure ~~SGIP~~IEIP effectively maintains and evolves the NSTIC ~~NIST Smart Grid~~Identity Ecosystem model~~Conceptual Model [8]~~ to provide more detail and depth so it can serve as a reference model for implementation architectures;

e. Engage and encourage Stakeholders to agree on a common path toward achieving ~~standards~~Ecosystem Framework standards-based interoperability using the conceptual and reference models;

f. Engage Stakeholders to encourage growth in the use of ~~standards~~Ecosystem Framework standards-based architectures and implementation designs; and

g. Oversee the ~~SGIP~~IEIP Testing and Certification Committee and framework.

h. [Other?]

### *1.5.2 ~~SGIPGB~~IEIPGB Activities*

The activities of the ~~SGIPGB~~IEIPGB will include, but not necessarily be limited to:

a. Affirming and ratifying ~~SGIP~~IEIP governing documents and operating procedures;

b. Provide guidance in establishing ~~SGIP~~IEIP procedures for recommending inclusion or exclusion of ~~standards~~Ecosystem Framework standards in the Interoperability Framework;

c. Provide guidance in establishing ~~SGIP~~IEIP procedures for producing recommended priority action plans and identifying recommended ~~standards~~Trust Framework standards;

d. Facilitating a testing and certification framework.

e. [Other?]

## 2. Bylaws

The Bylaws describe the roles, responsibilities, policies and procedures that govern the operation of the ~~SGIP~~IEIP. The Bylaws will be consistent with the framework of the Charge and Scope of this charter, which provide the high-level perspective of mission, purpose, and organization.

Operational materials, such as those describing active working groups, as well as the personnel involved in the ~~SGIP~~IEIP operation, will be made publicly available in companion documents.

### *2.1 ~~SGIP~~IEIP Roles and Responsibilities*

The ~~SGIP~~IEIP membership is open to all interested organizations,[1] as long as their interests fall within at least one of the Stakeholder Categories [NOTE: Consider whether unaffiliated individual members will be permitted to take part. If so, consider whether to create an

[1] An organization is defined as a commercial, governmental or other separately constituted legal entity and, when applicable its parent company or organization, its subsidiaries, affiliations, divisions, committees, and working groups.

unaffiliated individual category of stakeholder]. Divisions, subsidiaries, committees of organizations, etc. are part of their parent organizations, and are not considered organizations for ~~SGIP~~IEIP purposes. [NOTE: The foregoing provision appears intended to "consolidate" families and groups of entities for purposes of Steering Committee governance. The precise relationship of these definitions should be carefully correlated with the voting and other provisions of the charter to assure that the governance and decision making of the organization are consistent with stakeholder intentions] The composition and operation of the ~~SGIP~~IEIP should reflect~~have~~ a balance of interests. Participants from diverse interests will be sought with the objective of achieving balance; it being acknowledged that, while there might not be "perfect" balance in the view of a particular observer at any one time, an intention to achieve balance and the adoption of stakeholder information feedback mechanisms to enable nimble governance evolution will create a dynamic balance that can effectively "retune" the balance to seek broad stakeholder-responsive programs and results. For example, as the market matures, existing stakeholder groups represented in Exhibit A might reasonably be subdivided, combined or modified to reflect new market and community realities. This would be done at the initiation and with the agreement of the IEIP when and if warranted.

Stakeholder Categories that are recognized as necessary to achieve the goals of the ~~SGIP~~IEIP Categories are listed in Appendix A. Each Participating Member will be required to select a single Stakeholder Category for voting for ~~SGIPGB~~IEIPGB candidates. ~~SGIP~~IEIP members may participate in as many working groups as they have interest without regard to the category with which they are affiliated, provided that such participation will not alter the voting rights associated with membership set forth in section [ ].

*2.1.1 ~~SGIP~~IEIP Membership*

The ~~SGIP~~IEIP will have two (2) classes of members, Participating Members and Observer Members.

2.1.1.1 Participating Members

Participating Members are organizations who commit to participating in the work of the ~~Smart Grid~~Identity Ecosystem Interoperability Panel (~~SGIP~~IEIP)[NOTE Consider different name to reflect expanded scope of issues as discussed note accompanying section 1.1.4 above]. Participating Members will have the following rights and obligations:

a. The right to submit proposed requirements for the Identity Ecosystem Framework.

b. The right to participate in the ~~SGIP~~IEIP process and establish the overall direction for the ~~SGIP~~IEIP through active participation in Committees, or other ~~SGIP~~IEIP organizational teams as may be established from time to time by the ~~SGIP~~IEIP to address specific issues.

c. The right to vote on proposed ~~SGIP~~IEIP documents. Each Participating Member will be allocated one (1) vote on those ~~technical~~ matters that are proposed for a vote of the IEIP.[NOTE: Consider the scope of the voting ability. Note that the smart grid document limited voting in this section to "technical" matters.

Consider that the IEIP will work on technical and legal/policy matters.] That vote will be cast by an authorized Voting Member Representative. Voting rights are activated once a Participating Member has attended two consecutive meetings (face to face and/or web based). [NOTE: Consider the "types" of meetings that qualify to be included in this counting convention, i.e., is if "official" meetings, working meetings, etc.] (The only exception occurs during the first and second meeting of the ~~SGIP~~IEIP. See paragraph 2.1.1.1.d) Voting rights are temporarily and reversibly deactivated if a Participating Member has missed two consecutive meetings, whether face-to-face or web based, or document review and comment. The secretary for the ~~SGIP~~IEIP group that is meeting will keep attendance records for that meeting.

d. All Participating Members attending the first two meetings will be eligible to vote at those meetings. Thereafter for the ~~SGIP~~IEIP, paragraph 2.1.1.1.c takes effect.

e. The obligation to participate in ~~SGIP~~IEIP meetings.

f. The obligation to review ~~SGIP~~IEIP documents and provide comments.

g. The obligation to commit to participate in specific PAPs

h. The right to serve as a Participating Member for as long as they meet the requirements for membership. [NOTE: Consider whether there will be any limitation on participation based on objective criteria. Consider, for example, whether dues will be charged for membership (to support operations of the IEIP). If so, consider whether failure to pay dues will constitute grounds to suspend membership until member's dues account is brought current].

i. Each Participating Member may have multiple Member Representatives, but only one of those Member Representatives is allowed to vote on behalf of the Participating Member. This Member Representative may vote only on behalf of that Participating Member and may only cast one vote on any matter brought to a vote.

#### 2.1.1.2 Observer Members

Observer Members are Stakeholders that attend ~~SGIP~~IEIP meetings and review ~~SGIP~~IEIP documents, but do not commit to participating in the technical, legal and policy work of the ~~SGIP~~IEIP. Observer Members do not have the right to vote on ~~SGIP~~IEIP matters. Each Observer Member may have multiple Member Representatives.

#### 2.1.1.3 Membership Agreement

To become a Participating or Observer Member, each organization must sign an appropriate membership agreement that (1) states that the person signing the membership agreement has authority to enter into the agreement on behalf of their organization, and (2) that the organization will comply with the ~~SGIP~~IEIP Charter and Bylaws. The completed membership agreement is sent to the Administrator who collects and records the membership agreements. The

Participating Member may designate someone other than an employee to represent their organization. An individual may not be a Participating or Observer Member Representative for more than one Member Organization concurrently.

*2.1.2 Withdrawal*

Members can voluntarily withdraw from the ~~SGIP~~IEIP at any time by stating their intention in writing to the Secretary of the ~~SGIP~~IEIP, which withdrawal will be effective upon receipt by the Secretary of such notice.

*2.1.3 Replacement of Member Representatives*

If a Member Representative acts in a manner that interrupts the work of the ~~SGIP~~IEIP, the Participating Member may be asked to replace that Member Representative. If a Member Representative ceases to represent the Participating Member, the Participating Member must update their Membership Agreement.

*2.1.4 Stakeholder Representation*

A Stakeholder Category includes all Participating Members who have selected that Stakeholder Category. For voting purposes, each Participating Member is allotted one vote. This will serve to help ensure that no single interest dominates the process or is favored over another among competing interests and various Stakeholder Categories.

*2.1.5 ~~SGIP~~IEIP Officers*

**Plenary Chair**:

a. The Plenary Chair is elected by a majority vote of the ~~SGIPGB~~IEIPGB.

b. Duties. The Chair will facilitate ~~SGIP~~IEIP meetings. The Chair is responsible for establishing meeting schedules, agendas, business to be conducted, and coordinates the speakers to lead presentations and discussions. The Chair will manage disputes, and is responsible for fostering an open, friendly atmosphere at ~~SGIP~~IEIP conferences and meetings. The Chair is responsible for assigning and tracking ~~SGIP~~IEIP action items, risks, and issues.

c. Term of Service. The Chair will serve a two-year term; the Chair may be re-elected by the ~~SGIPGB~~IEIPGB for one consecutive two-year term. The Chair may serve no more than two terms consecutively. The Chair can serve multiple non-consecutive terms. If the Chair is unable to complete his/her term of office, the ~~SGIPGB~~IEIPGB will select a successor. The Plenary Chair will have authority to table or terminate discussion, call for affirmation of consensus, mediate with dissenting parties or recommit a matter to committee for further action.

d. The Plenary Chair may be removed by a 75% (three-fourths) super-majority vote or greater of the ~~SGIPGB~~IEIPGB.

e. The Plenary Chair will only vote on matters before the ~~SGIP~~IEIP in cases of a tie.

**Plenary Vice Chair**:

a. The Plenary Vice Chair will be elected by a simple majority vote of the Stakeholders that comprise the ~~SGIP~~IEIP.

b. Duties. The Vice Chair will support the Plenary Chair in performing the Plenary Chair's duties, and ensure that meeting minutes, notes, and other meeting artifacts are posted and available to ~~SGIP~~IEIP members. The Plenary Vice Chair will serve as Chair at meetings where the Chair cannot attend.

c. Term of Service. The Vice Chair will serve a two-year term; the Vice Chair may be reelected by the ~~SGIP~~IEIP for one consecutive two-year term. The Vice Chair may serve no more than two terms consecutively. If the Vice-Chair is unable to complete his/her term of office, the ~~SGIP~~IEIP will elect a successor.

**Plenary Secretary**:

a. The Plenary Secretary will be nominated and elected by majority vote of the ~~SGIP~~IEIP.

b. Duties. The Plenary Secretary will provide all administrative support services to the ~~SGIP~~IEIP membership, including but not limited to: scheduling meetings, notifying members of ~~SGIP~~IEIP meetings, preparing agendas, and recording and posting minutes. The Plenary Secretary will post proposed additions and deletions to the OIX Online Knowledge Base~~Interoperability Knowledge Base (IKB)~~ upon approval of the ~~SGIP~~IEIP.

c. Term of Service. The Plenary Secretary will serve a term of two years; the Plenary Secretary may be reelected by the ~~SGIP~~IEIP for one consecutive two-year term. The Plenary Secretary may serve no more than two terms consecutively. If the Plenary Secretary is unable to complete his/her term of office, the ~~SGIP~~IEIP will elect a successor.

### *2.1.6 Administrator and Support Resources*

The role of the Administrator will be as follows:

a. The Administrator will manage the internal operation of the ~~SGIP~~IEIP.

b. The Administrator will arrange human and financial resources in support of ~~SGIP~~IEIP activities. This will include:

- Meeting arrangements,
- Interactions with other organizations, and

- Other activities needed by the ~~SGIP~~IEIP

The Administrator will initially be selected as a [NOTE: Discuss and include reference to initiation and the role of the administrator]. ~~NIST contractor. The NIST contract~~[ ] will initially provide the financial support for this function. [NOTE: discuss and reference funding here.] The Administrator is an ex officio non-voting member of the ~~SGIPGB~~IEIPGB. [NOTE: Consider whether and how OIX programs, tools and resources can be enlisted to help with administration of the IEIP]

### *2.1.7 Meetings and Decision Making*

Except as otherwise noted, the ~~SGIP~~IEIP and ~~SGIPGB~~IEIPGB, and all working groups and committees will meet and make decisions as follows:

a. Meetings and decision-making will be presided over by the respective Chair.

b. Attendance will be recorded for all meetings.

c. Formal discussion and decision-making procedures will follow Robert's Rules of Order Newly Revised Version.[2]

d. The intellectual property disclosure policy (see Section 2.6 "Intellectual Property") and the description of activities that violate anti-trust law (see Section 2.9 "Competition") will be reviewed at the start of every meeting.

e. The ~~SGIP~~IEIP and the ~~SGIPGB~~IEIPGB will hold face-to-face meetings each meet at least two times per year, with all meetings (including the face-to-face meetings) providing the opportunity for members and the public to attend via the web.

f. There will be no defined limit on the maximum number of meetings. Meeting scheduling is left to the discretion of the involved working group or other ~~SGIP~~IEIP organizational unit. All ~~SGIP~~IEIP and ~~SGIPGB~~IEIPGB meetings will include web based access for attendance by members and the public unable to travel.

g. Draft minutes of meetings will be distributed to the appropriate Members for comment and revised accordingly; the minutes will be approved by a simple majority of the appropriate Members. Minutes should be made publicly available as soon as possible after a particular meeting.

h. Decisions may be reached by face-to-face meeting, teleconference, electronic communication, or any combination of the above.

i. Revisions to these Bylaws by the ~~SGIP~~IEIP will be adopted through this process.

[2] *Robert's Rules of Order Newly Revised*, 10th edition, Perseus Books Group, Cambridge MA, 2000.

#### 2.1.7.1 Meeting Place

All meetings of the Members will be held at such place as will be determined from time to time by the ~~SGIP~~IEIP, and the place at which any such meeting will be held will be stated in the notice of the meeting. All meetings will include the option to attend via the web. Meetings can be in the form of teleconferences and web meetings.

#### 2.1.7.2 Open Meetings; Notice

~~SGIP~~IEIP meetings and minutes are open and available to the public. Meetings of the ~~SGIP~~IEIP will be announced not less than 30 calendar days prior to in-person meetings and not less than 10 calendar days prior to virtual meetings. Notifications will be communicated by email to ~~SGIP~~IEIP membership and by posting on the ~~SGIP~~IEIP web site. This meeting notice does not apply to meetings of ~~SGIP~~IEIP committees or working groups.

#### 2.1.7.3 Prior Publication and Review of ~~SGIP~~IEIP Matters

Announcements of ~~SGIP~~IEIP meetings will include the date and time for the meeting, the subject matter and agenda. A description of any matter to be put to a vote of the ~~SGIP~~IEIP will be included in the meeting notice, including the recommendation of the working group and web links to any working papers. Prior to any formal vote on any matter

recommended to the ~~SGIP~~IEIP, working group papers and documents will be posted on the ~~SGIP~~IEIP web site [and OIX Knowledge Center] for public comment and there will be at least a ten (10) business day review and comment period.

#### 2.1.7.4 Attendance

Attendance at ~~SGIP~~IEIP meetings is an obligation of membership. The Plenary Secretary will record the presence of each Member at each ~~SGIP~~IEIP meeting (both in person and via telepresence over web, phone or other electronic means). It will be the responsibility of ~~SGIP~~IEIP Members to make their attendance at ~~SGIP~~IEIP meetings known to the Secretary. This attendance requirement only applies to meetings of the ~~SGIP~~IEIP as a whole.

#### 2.1.7.5 Quorum

A simple majority of all Participating Members will be necessary and sufficient to constitute a quorum for the transaction of business.

#### 2.1.7.6 Manner of Acting

At a meeting at which a quorum is achieved, the affirmative vote of seventy-five percent (75%) of the quorum will be the act of the ~~SGIP~~IEIP with regard to technical, legal or policy matters associated with Trust Framework standards. [NOTE: Where voting rules are involved, it will be helpful to provide specific, objective tests of application. Thus, it will be important to state with some precision when an issue is considered to be "technical, legal or policy" requiring a 75% vote. A first suggestion is to add the modifier "associated with Trust Framework standards" to help clarify, but additional guidance will be useful in determining when a supermajority vote is

required for group action].Administrative matters may be decided by a simple majority of the quorum. [NOTE: See comment immediately above for issues of "dividing" line between majority and supermajority votes] For Governing Board member elections requirements see section 2.2.2.1.5.

### *2.2 ~~SGIPGB~~IEIPGB Roles and Responsibilities*

#### *2.2.1 ~~SGIPGB~~IEIPGB Membership*

The ~~SGIPGB~~IEIPGB will consist of [twenty-seven (27)][NOTE: Insert number here that reflects stakeholder count plus other members in the Identity Ecosystem context] members, including a Chair and [NOTE: Insert prior number less one][twenty-six (26) members], purposefully selected to represent a spectrum of industry expertise and Stakeholder Categories relevant to the ~~Smart Grid~~Identity Ecosystem. The membership will be as follows:

a. [Twenty-two (22)][NOTE: Insert appropriate number] of the ~~SGIPGB~~IEIPGB members will include a Member from each of the identified [twenty-two (22)] [NOTE: Insert appropriate number] Stakeholder Categories identified ~~by NIST. The Stakeholder Categories are listed~~ in Appendix A.

Note: Since the IEIPGB membership is constituted based on the various stakeholder categories, it is crucial that care be taken to aggregate stakeholder categories appropriately to avoid inadvertent duplicative or derivative stakeholder categories that might cause an imbalance in voting rights in the IEIPGB. Such an imbalance could ultimately undercut the intentions of the Identity Ecosystem to promote wide scale adoption and sustainability, and should be avoided.

In addition, initial definition of stakeholder categories should be prioritized to enable, in particular, stakeholder categories that recognize various online e-commerce stakeholders in support of a key goal of NSTIC to promote economic growth both in the U.S. and internationally.

b. Two (2) ~~SGIPGB~~IEIPGB members will include the Chair of the ~~Smart Grid~~Identity Ecosystem Architecture Committee (~~SGAC~~IEAC) and the Chair of the ~~Smart Grid~~Identity Ecosystem Testing and Certification Committee (~~SGTCC~~IETCC). (See paragraphs 2.3.1 and 2.3.2). These positions on the ~~SGIPGB~~IEIPGB will remain vacant until the ~~SGAC~~IEAC and ~~SGTCC~~IETCC are formed and their Chairs selected.

c. The remaining three (3) members will be elected "at large ".

d. The NIST National Coordinator for NPO~~Smart Grid~~ and the Administrator will serve as ex officio non-voting members of the ~~SGIPGB~~IEIPGB. Additional ex officio non-voting members can be invited by vote of the ~~SGIPGB~~IEIPGB. See

section 2.2.2.2. [NOTE: Consider other organizations that interact with the IEIP and IEIPGB for which ex officio membership would be appropriate]

e. All ~~SGIPGB~~IEIPGB voting members will qualify to hold an officer position within the ~~SGIPGB~~IEIPGB.

*2.2.2 Selection of ~~SGIPGB~~IEIPGB Members*

2.2.2.1 Selection of Voting Members

*2.2.2.1.1 Call for Candidates*

When one or more seats become open on the ~~SGIPGB~~IEIPGB, the Chair will request that the Administrator launch a Call for Candidates as follows:

a. The request will indicate the number of member seats to be filled and provide guidance on specific candidate attributes which may be needed to fulfill ~~SGIPGB~~IEIPGB requirements for skills, experience, and cross-industry representation.

b. Any ~~SGIP~~IEIP Participating Member may submit a recommendation in response to the Call for Candidates, with the exceptions noted in paragraph (c).

c. For Stakeholder Category positions, only members of that Stakeholder Category may recommend a candidate for the open position.

d. For the initial ~~SGIPGB~~IEIPGB, the Administrator will launch the Call for Candidates when requested by [NOTE: Insert appropriate entity here. Head of the NPO?] ~~NIST~~.

*2.2.2.1.2 Candidate Evaluation Committee*

To evaluate responses to the Call for Candidates, the Administrator will propose a Candidate Evaluation Committee as follows:

a. The proposed Candidate Evaluation Committee will consist of eight (8) individuals, selected based on their breadth of experience, their contributions to the ~~Smart Grid~~Identity Ecosystem Community, and their history of a balanced approach to addressing ~~Smart Grid~~Identity Ecosystem issues.

b. The proposed Candidate Evaluation Committee will include at least three (3) ~~SGIPGB~~IEIPGB members whose terms are not expiring.

c. [NOTE: Consider whether the following is appropriate given the more limited role of the government in the Identity Ecosystem steering committee. If so, consider a time limitation such as that suggested below.][One member of the Candidate Evaluation Committee during the first two (2) years of Steering Committee Operation) will be the NPO~~IST National Coordinator for Smart Grid~~

~~Interoperability~~ representative as an ex officio member. ~~He or she may delegate this role to another NIST staff working on behalf of NIST~~]

d. The proposed Candidate Evaluation Committee will be subject to approval by a vote of the ~~SGIPGB~~IEIPGB according to the normal decision-making process.

e. For the initial ~~SGIPGB~~IEIPGB, the Administrator will assume the responsibilities of the Candidate Evaluation Committee.

f. The Candidate Evaluation Committee will evaluate responses to the Call for Candidates against the following ~~NIST-developed~~ eligibility criteria:

i. Visionary Capability: ~~SGIPGB~~IEIPGB Members will be capable of understanding and contributing to the multi-disciplinary aspects of the ~~Smart Grid~~Identity Ecosystem and the specific goals of the ~~SGIP~~IEIP mission.

ii. Team Effectiveness: ~~SGIPGB~~IEIPGB Members will be capable of working effectively as a team within the scope of the ~~SGIPGB~~IEIPGB.

iii. Outreach: ~~SGIPGB~~IEIPGB Members will be able to relay and leverage ~~SGIPGB~~IEIPGB messages through the stakeholder community, contributing to underlying consensus building goals of the ~~SGIPGB~~IEIPGB.

iv. Recognition: ~~SGIPGB~~IEIPGB Members will be recognized experts in their technical fields of endeavor

v. Commitment: Members will be committed to contribute time and effort to ~~SGIPGB~~IEIPGB activities.

*2.2.2.1.3 Preparation of a Slate*

a. The Candidate Evaluation Committee will verify the eligibility of candidates, including their ability to fulfill the requirements of the open seats.

b. The Candidate Evaluation Committee will develop a slate of all eligible candidates from all candidate nominations received during the Call for Candidates, corresponding to the requirements for vacant seats.

c. Candidates may only appear once on a slate.

*2.2.2.1.4 Confirmation of a Slate*

a. The slate will be defended by the Candidate Evaluation Committee before the sitting ~~SGIPGB~~IEIPGB.

b. Except for the nominations for the initial ~~SGIPGB~~IEIPGB, the sitting ~~SGIPGB~~IEIPGB will vote to accept or reject the slate or individual nominees within the slate, as appropriate. Individual nominees may only be rejected by the ~~SGIPGB~~IEIPGB if they do not meet the eligibility criteria or they are otherwise not qualified to fill the open position for which they are nominated.

c. Cause for rejection will be clearly stated so that the Candidate Evaluation Committee may propose a new slate or a partial slate.

*2.2.2.1.5 Election of ~~SGIPGB~~IEIPGB Members*

Election of ~~SGIPGB~~IEIPGB members will be as follows:

a. Only Participating Members of a Stakeholder Category may vote for Candidates being elected from that Stakeholder Category.

b. ~~SGIPGB~~IEIPGB members who are the Chairs of the ~~Smart Grid~~Identity Ecosystem Architecture Committee and the Chair of the ~~Smart Grid~~Identity Ecosystem Testing and Certification Committee will be selected according to section 2.3.1 and 2.3.2, respectively.

c. All Participating Members of the ~~SGIP~~IEIP may vote for Candidates being elected for "at large" positions.

d. Candidates are elected by the highest vote count of the Stakeholders voting for that position.

e. Should seats remain open at the end of the confirmation process, the Chair may provide guidance to the Administrator to initiate another Call for Candidates.

f. A tie vote will result in another ballot conducted in a timely fashion, involving only the tied candidates.

2.2.2.2 Ex Officio Non-Voting Members

The following are ex officio non-voting members of the ~~SGIPGB~~IEIPGB:

a. The NPO Representative~~NIST National Coordinator for Smart Grid~~, who may delegate service on the ~~SGIPGB~~IEIPGB to another NIST employee.

b. The ~~SGIP~~IEIP Administrator.

c. The ~~SGIP~~IEIP Plenary Chair

d. The ~~SGAC~~IEAC Chair

e. The ~~SGTCC~~IETCC Chair

f. [Other?]

~~f.~~g. Additional ex officio members as may be added or removed from the current list by the ~~SGIPGB~~IEIPGB by a simple majority vote of the board.

2.2.2.3 Ex Officio Non-Voting Member Participation

a. Ex officio non-voting members will attend all ~~SGIPGB~~IEIPGB meetings.

b. Ex officio non-voting members will have no standing to participate in ~~SGIPGB~~IEIPGB decisions but may participate in ~~SGIPGB~~IEIPGB discussions as appropriate to their roles.

2.2.2.4 Standing Invitee

The ~~SGIPGB~~IEIPGB may by a simple majority vote issue a standing invitation to an organization or individual to observe ~~SGIPGB~~IEIPGB activities. Standing invitees cannot vote in the ~~SGIPGB~~IEIPGB, but may participate in ~~SGIPGB~~IEIPGB discussions.

*2.2.3 Duties of ~~SGIPGB~~IEIPGB Members*

a. Once elected ~~SGIPGB~~IEIPGB Members will serve as individuals and not as representatives of any company, agency, stakeholder category or other organization.

b. ~~SGIPGB~~IEIPGB Members will owe no fiduciary duty of loyalty or care to the ~~SGIPGB~~IEIPGB or the ~~SGIP~~IEIP.

If an ~~SGIPGB~~IEIPGB Member was a Voting Member Representative for their Participating Member prior to their election, the Participating Member must designate a new Voting Member Representative by updating their Membership Agreement.

When participating in ~~SGIPGB~~IEIPGB activities, members' primary consideration must be the impact of an ~~SGIPGB~~IEIPGB decision on the public interest and on the economic and operational reliability, integrity, [NOTE: List other desirable characteristics here] security of the ~~Smart Grid~~Identity Ecosystem.

*2.2.4 Terms of ~~SGIPGB~~IEIPGB Membership*

Members will be selected according to the procedures defined in paragraph 2.2.2. The terms of Members will be as follows:

a. Members of the ~~SGIPGB~~IEIPGB will serve two-year terms. For the initial ~~SGIPGB~~IEIPGB, the SGIPBG Members of the even numbered Stakeholder Categories listed in Appendix A will serve a one-year term, and the ~~SGIPGB~~IEIPGB Members of the odd numbered Stakeholder Categories listed in Appendix A will serve a two-year term. The initial at-large ~~SGIPGB~~IEIPGB members will serve two year terms.

b. The start of the membership selection process will occur annually in mid-September with renewed and new Members targeted to be in place by January 1.

c. A member starting before July 1 is deemed to have a term starting on January 1 of that year.

d. A member starting on or after July 1 is deemed to have a term starting on January 1 of the following year.

e. Member terms will expire on December 31 of their second year. For the initial ~~SGIPGB~~IEIPGB, the terms of one-year Members will expire on December 31 of their first year.

f. There is no limit to the number of terms ~~SGIPGB~~IEIPGB Members may serve.

g. Mid-term vacancies will be filled as described below and will not affect the ~~SGIPGB~~IEIPGB's ability to take decisions.

*2.2.5 Ending Membership*

a. A Member may complete a term, or relinquish membership voluntarily.

b. Upon termination of a member, a replacement must be chosen by selection at the earliest reasonable opportunity,

c. Should a Member become unable to fulfill their commitment, they will be expected to vacate their seat.

*2.2.6 Officers*

The ~~SGIPGB~~IEIPGB Officers will include a Chair, Vice Chair and Secretary. If consensus is not achieved when voting for an officer position other than the Chair then the process outlined in paragraph 2.2.7, Meetings and Decision Making, will be followed.

2.2.6.1 Chair

*2.2.6.1.1 Chair Selection*.

The Chair will be selected from among the ~~SGIPGB~~IEIPGB membership by simple majority vote of the ~~SGIPGB~~IEIPGB membership ~~and confirmed by the NIST National Coordinator for Smart Grid Interoperability (NCSGI)~~ as follows:

a. The Administrator will initiate the selection with a call for Chairperson Nominations.

b. The call for nominations may be issued up to three months prior to any expected vacancy in the Chair position.

c. Candidates for Chair will be sitting members of the ~~SGIPGB~~IEIPGB.

d. To be considered, Candidates must be nominated by two members prior to the vote for Chair. The criteria for nomination and for selection are:

i. Breadth of experience

ii. Contributions to the ~~Smart Grid~~Identity Ecosystem community

iii. History of a balanced approach to addressing ~~Smart Grid~~Identity Ecosystem issues

iv. Demonstrated ability to effectively lead a significant organization or an organization board.

e. The ~~SGIPGB~~IEIPGB will elect a Chair from among the nominees by a vote of the ~~SGIPGB~~IEIPGB membership following the voting rules in section 2.2.7, Meetings and Decision Making.

~~e.The elected Chair will be submitted by the Administrator to the NIST National Coordinator for Smart Grid (NIST NCSGI) for confirmation.~~

~~g.~~f. ~~In the event that the NIST NCSGI does not confirm the elected Chair, the NIST NCSGI must provide clear reasons why he/she does not believe the recommended Chair meets the criteria to the SGIPGB and allow the SGIPGB to submit another recommendation for Chair.~~

*2.2.6.1.2 Responsibilities*

The Chair will:

a. Act as a lead spokesperson for the ~~SGIPGB~~IEIPGB between meetings.

b. Be the primary point of contact for coordination with the Administrator for the arrangement of meetings and planning of activities.

c. The ~~SGIPGB~~IEIPGB Chair shall only vote on matters before the ~~SGIPGB~~IEIPGB in cases of a tie.

*2.2.6.1.3 Term*

The term of the Chair will be one year, with no restriction on the number of consecutive terms.

2.2.6.2 Vice Chair

The Vice Chair will be nominated and elected by a vote of the ~~SGIPGB~~IEIPGB following the voting rules in section 2.2.7, Meetings and Decision Making. The Vice Chair will support the Chair in performing the Chair's duties, and will ensure that meeting minutes, notes, and other meeting artifacts are posted and available to members. The Vice Chair will serve as chair at meetings where the Chair cannot attend. The Vice Chair will serve a term of one year with no restriction on the number of consecutive terms.

#### 2.2.6.3 Secretary

A Secretary will be nominated and elected by a simple majority vote of the ~~SGIPGB~~IEIPGB. The Secretary will serve a term of one year with no restriction on the number of consecutive terms.

### *2.2.7 Meetings and Decision Making*

a. The ~~SGIPGB~~IEIPGB will meet and make decisions in accordance with paragraph 2.1.7, Meetings and Decision Making.

b. If consensus is not achieved, the ~~SGIPGB~~IEIPGB may make decisions and take action if at least [NOTE: Adjust the following numbers based on the number of stakeholder groups in the Identity Ecosystem Steering Committee context][fourteen (14)] full members concur and there are no more than [six (6) dissenting votes].

#### 2.2.7.1 Meeting Place

All meetings of the ~~SGIPGB~~IEIPGB Members will be held at such place as will be determined from time to time by the ~~SGIPGB~~IEIPGB, and the place at which any such meeting will be held will be stated in the notice of the meeting.

#### 2.2.7.2 Open Meetings; Notice

~~SGIPGB~~IEIPGB meetings and minutes are open and available to the public. Except for the initial meeting of the ~~SGIPGB~~IEIPGB, meetings of the ~~SGIPGB~~IEIPGB will be announced not less than 30 calendar days prior to in-person meetings and no less than 10 calendar days prior to virtual meetings. Notifications will be communicated by email to ~~SGIPGB~~IEIPGB membership and by posting on the ~~SGIP~~IEIP web site.

#### 2.2.7.3 Prior Publication and Review of ~~SGIPGB~~IEIPGB Matters

Announcements of ~~SGIPGB~~IEIPGB meetings will include the date and time for the meeting, the subject matter and the agenda. A description of any matter to be put to a vote of the ~~SGIPGB~~IEIPGB will be included in the meeting notice, including the recommendation of the working group and web links to any working papers. Prior to any formal vote on any matter recommended to the ~~SGIPGB~~IEIPGB, working group papers and documents will be posted on the ~~SGIPGB~~IEIPGB web site [NOTE: Consider whether the OIX Knowledge Center might also be made available to assure broad dissemination of materials]for public comment and there will be at least a ten (10) business day review and comment period.

#### 2.2.7.4 Attendance

Attendance at ~~SGIPGB~~IEIPGB meetings is an obligation of ~~SGIPGB~~IEIPGB membership. The ~~SGIPGB~~IEIPGB Secretary will record the presence of each Member at each ~~SGIPGB~~IEIPGB meeting. Every Member must make a concerted effort to attend all meetings (face-to-face

meetings and web conferences). Missing two out of four consecutive meetings will be grounds, but not a requirement, for a vote to remove the Member from the ~~SGIPGB~~IEIPGB.

#### *2.2.8 Quorum*

A simple majority of all Members will be necessary and sufficient to constitute a quorum for the transaction of business.

### *2.3 ~~SGIP~~IEIP Standing Committees*

The ~~SGIP~~IEIP may establish standing committees, to address cross-industry group issues or other ~~SGIP~~IEIP priority areas, subject to approval of the ~~SGIPGB~~IEIPGB.

At a minimum, the ~~SGIP~~IEIP will maintain the following standing committees:

- ~~Smart Grid~~Identity Ecosystem Architecture Committee
- ~~Smart Grid~~Identity Ecosystem Testing and Certification Committee

Additional committees will be established as necessary by the ~~SGIP~~IEIP with the approval of the ~~SGIPGB~~IEIPGB.

There will be no limit on the number of Standing Committee members, although a target of 30 members may be considered for most committees.

The Secretary for each individual committee will be responsible for the committees they serve to schedule meetings, prepare agendas, recording and posting of meetings. The Secretary for an individual committee will be nominated and elected by majority vote of that committee.

#### *2.3.1 ~~Smart Grid~~Identity Ecosystem Architecture Committee*

The ~~Smart Grid~~Identity Ecosystem Architecture Committee (~~SG~~IEAC) is responsible for creating and refining a conceptual reference model, including lists of the ~~standards~~Trust Framework standards and profiles necessary to implement the vision of the ~~Smart Grid~~Identity Ecosystem [NOTE: Review the foregoing responsibilities and modify as necessary to reflect required functions here]. The ~~SG~~IEAC will include at least eight Members selected by the Plenary Chair, and all other interested members confirmed by majority vote of the ~~SGIP~~IEIP.

The ~~SGAC~~IEACIEAC Chair will also serve as a non-voting member of the ~~SGIPGB~~IEIPGB and, therefore, must meet the criteria for service on the ~~SGIPGB~~IEIPGB. The Plenary Chair will select the ~~SGAC~~IEACIEAC Chair from among the ~~SGAC~~IEACIEAC members and will submit the selected Chair to the ~~SGIPGB~~IEIPGB for confirmation.

The ~~SGAC~~IEACIEAC Vice Chair and Secretary will be selected by a majority vote of the ~~SGAC~~IEACIEAC. All ~~SGAC~~IEAC Officers will serve two-year terms, with no restrictions on serving consecutive terms. If the Vice Chair or Secretary is unable to complete his/her term of office, the Plenary Chair will select a successor.

### *2.3.2 ~~Smart Grid~~Identity Ecosystem Testing and Certification Committee*

The ~~Smart Grid~~Identity Ecosystem Testing and Certification Committee (~~SG~~IETCC) will consist of at least eight members selected by the Plenary Chair, and all other interested members confirmed by majority vote of the ~~SGIP~~IEIP. The ~~SGTCC~~IETCC creates and maintains the necessary documentation and organizational framework for compliance, interoperability and cyber security testing and certification for ~~SGIP~~IEIP-recommended ~~Smart Grid~~Identity Ecosystem ~~standards~~Trust Framework standards [NOTE: Review the foregoing responsibilities and modify as necessary to reflect required functions here].

The ~~SGTCC~~IETCC Chair will also serve as a non-voting member of the ~~SGIPGB~~IEIPGB and, therefore, must meet the criteria for service on the ~~SGIPGB~~IEIPGB. The Plenary Chair will select the ~~SGTCC~~IETCC Chair from among the ~~SGTCC~~IETCC members and will submit the selected Chair to the ~~SGIPGB~~IEIPGB for confirmation.

~~The SGTCC Vice Chair will be a NIST staff person.~~

The ~~SGTCC~~IETCC Secretary will be selected by a majority vote of the ~~SGTCC~~IETCC. The ~~SGTCC~~IETCC Officers will serve two-year terms, with no restrictions on serving consecutive terms. If the Secretary is unable to complete a full term of office, the Plenary Chair will select a successor.

The Standing Committee Chairs will only vote within their committee for cases of a tie.

## *2.4 Working Groups*

The ~~SGIP~~IEIP may create working groups and other subgroups as deemed necessary to address a specific problem or work product, such as but not limited to a Priority Action Plan (PAP), to accomplish its charge. Each working group and subgroup will have a charter document prepared stating the goals for the group. Each subgroup will elect a Chair, Vice-Chair, and Secretary from among ~~SGIP~~IEIP Participating Members. They will operate autonomously to achieve their stated goals. [NOTE: Consider mention of coordination with OIX working groups here. Consider whether OIX might provide the infrastructure to support Steering Committee working groups. Consider preparation of default provisions for operations of working groups to facilitate formation (see OIX Member Rules Part VI (confirm cite) for example).]

The Chair of a subgroup will prepare a report on the status, plans, and schedule of the subgroup for every face to face meeting of the ~~SGIP~~IEIP and as called upon for electronic conference sessions. The Chair of a subgroup will determine if other officer positions are necessary and will fill those positions by appointment.

It is expected that working groups and subgroups will meet primarily through teleconferences and web-based meetings. If face-to-face meetings are held, an opportunity for web-based attendance will be provided.

The ~~SGIP~~IEIP will decide when to disband Working Groups and other subgroups, except for the ~~Smart Grid~~Identity Ecosystem Cyber Security Working Group (CSWG), which will be a permanent working group.

The Working Group Chairs shall only vote within their working group for cases of a tie.

#### *2.4.1 ~~Smart Grid~~Identity Ecosystem Cyber Security Working Group*

The ~~Smart Grid~~Identity Ecosystem Cyber Security Working Group (IE~~SGCSWG~~IECSWG) will be a permanent working group that provides expertise needed to address matters related to cyber security for the ~~Smart Grid~~Identity Ecosystem. It plays a critical role in identifying the ~~standards~~Trust Framework standards and architecture needed to ensure the security of the Identity Ecosystem~~smart grid~~, which is a critical national infrastructure.

#### *2.4.2 Identity Ecosystem Identity Integrity Working Group*

The Identity Ecosystem Identity Integrity Working Group (IEIIWG) will be a permanent working group that provides expertise needed to address matters related to privacy, identity integrity and related matters for the Identity Ecosystem. It plays a critical role in identifying the Trust Framework standards and architecture needed to ensure the integrity of identity and privacy in the Identity Ecosystem, which is a critical national infrastructure.

~~The SGCSWG Chair will be a NIST staff person.~~

### *2.5 ~~SGIP~~IEIP Voting*

#### *2.5.1 What May Be Voted Upon*

Votes may occur on any issue that will be presented.

#### *2.5.2 Who May Vote*

Participating Members who have not been absent from two consecutive meetings may vote.

#### *2.5.3 Voting Process*

A Working Group must vote to pass a measure prior to presenting it to the ~~SGIP~~IEIP. The ~~SGIP~~IEIP must vote to pass a measure prior to presenting it to the ~~SGIPGB~~IEIPGB.

Initially, the ~~SGIP~~IEIP, its ~~SGIPGB~~IEIPGB and its committees and working groups will attempt to achieve consensus on matters before them. If unable to reach consensus, a vote will be taken.

All Participating Members with at least one Member Representative on a particular Working Group can participate in that Working Group's votes. For that Working Group's vote only, each Participating Member must designate only one (1) Member Representative to vote on its behalf. This designated Member Representative need not be the Voting Member Representative.

#### *2.5.4 Absence; Restoration of Voting Privilege:*

Any Participating Member who is (1) absent for two consecutive meetings or (2) does not vote in two consecutive meetings in which voting occurs, will forfeit the privilege of voting on any matter. The attendance record of Participating Members will be kept in an online database. A Participating Member whose voting privileges are suspended will have voting privileges restored

upon attendance at two consecutive meetings. Restoration of voting privileges begins after determination of quorum at the second consecutive meeting attended. All Participating Members attending the first two meetings will be eligible to vote at those meetings. Thereafter for the ~~SGIP~~IEIP, paragraph 2.1.1.1 takes effect.

When making decisions each Participating Member is allotted one vote.

*2.5.5 When a Vote May Occur*

Votes may occur at any meeting announced in accordance with these Bylaws and on any matter advertised in the meeting notice.

*2.5.6 Record of Voting*

A record of voting on all measures requiring a vote will be kept on the web site. Votes may either be:

a. "Yes",

b. "Yes, with comment",

c. "No, with comment," or

d. "Abstain".

All "No" votes must be accompanied by written comments to document why that position was taken and that vote cast.

*2.5.7 Requirements for Passing*

Seventy-five percent (75%) of the quorum must approve a technical, legal or policy [NOTE: Conform this expanded set to the approach taken in section 1.4.4.] measure for it to pass. A simple majority of the quorum is required for passage of administrative matters. A quorum is described below. "Abstain," votes will be subtracted from the denominator in the percentage approval calculation.

*2.5.8 Quorum*

A Quorum of the ~~SGIP~~IEIP is defined as greater than fifty percent (50%) of Participating Members eligible to vote.

*2.5.9 Voting within a Stakeholder Category*

For the election of a ~~SGIPGB~~IEIPGB candidate within a Stakeholder Category, only Participating Members within that Stakeholder Category may vote.

Each Participating Member is permitted to cast one vote.

#### *2.5.10 Electronic Voting*

The ~~SGIP~~IEIP, ~~SGIPGB~~IEIPGB and each Committee or Working Group will conduct electronic balloting on issues within their purview. A standard voting mechanism will be used that logs votes for audit, verifies a quorum is attained and prevents "flooding" of votes by a Member.

### *2.6 Intellectual Property*

[NOTE: Consider whether the following should be refined or expanded in the identity Ecosystem context]The ~~SGIP~~IEIP policy related to Intellectual Property is based on the following principles:

a. The ~~SGIP~~IEIP, the ~~SGIPGB~~IEIPGB, all committees and all working groups and subgroups function in an open working environment. The ~~SGIP~~IEIP and its Members will not accept any documentary or oral disclosure of confidential or proprietary information from any Member as a part of the ~~SGIP~~IEIP's conduct of business. In addition, no information of a secret or proprietary nature will be made available to the ~~SGIP~~IEIP as official documents, and no such documents (or documents marked as such) will be made ~~SGIP~~IEIP official documents or forwarded to the membership.

b. All proprietary information which may nonetheless be publicly disclosed by any participant during any meeting of the ~~SGIP~~IEIP, the ~~SGIPGB~~IEIPGB or its committees or working groups will be deemed to have been disclosed on a non-confidential basis, without any restrictions on use by anyone, except that no valid copyright or invention right will be deemed to have been waived by such disclosure.

#### *2.6.1 ~~SGIP~~IEIP Patent Policy - Inclusion of Patents in ~~SGIP~~IEIP-Identified Products*

Some ~~SGIP~~IEIP-identified Ecosystem Framework standards and other outputs~~product~~ may require~~include~~ the use of an essential patent claim (one whose use would be required for compliance with that standard) if technical reasons justify this approach. If ~~SGIP~~IEIP receives a notice that a proposed or an approved ~~SGIP~~IEIP product may require the use of such a patent claim, the procedures in the following sections will be followed.

#### *2.6.2 Statement from Patent Holder*

The ~~SGIP~~IEIP will request from the patent holder or a party authorized to make assurances on its behalf, in written or electronic form an assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of implementing the ~~SGIP~~IEIP product either:

a. On a non discriminatory basis and under reasonable terms and conditions; or

b. Without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

If the patent holder or party authorized to make assurances on its behalf does not agree to these terms, then this decision will be documented clearly. As it may pose risks to the implementation of the ~~Smart Grid~~Identity Ecosystem, this decision will be seriously considered by the ~~SGIP~~IEIP in any related activity or vote.

2.6.2.1 Record of Statement

A record of the patent holder's statement will be retained in the ~~SGIP~~IEIP files and posted on-line.

2.6.2.2 Notice

When the ~~SGIP~~IEIP receives from a patent holder the assurance set forth in 2.6.1 above, the expected result will include a note to be included in the Trust Framework ecosystem documentation to read substantially as follows:

NOTE — The user's attention is called to the possibility that compliance with this expected result may require use of an invention covered by patent rights.

By publication of ~~SGIP~~IEIP expected results, no position is taken with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under section 2.6.1, details may be obtained from the patent holder.

2.6.2.3 Responsibility for Identifying Patents

Neither the ~~SGIPGB~~IEIPGB nor ~~SGIP~~IEIP is responsible for identifying patents for which a license may be required for use of an ~~SGIP~~IEIP expected result or for conducting inquiries into the legal validity or scope of those patents that are brought to their attention.

*2.6.3 Copyrights*

Copyright in materials produced prior to Membership in the ~~SGIP~~IEIP remains the property of the copyright owner. However, copyrighted materials offered for incorporation into ~~SGIP~~IEIP outputs must be made available on a royalty-free basis. Members who contribute to IEIP~~SIGP~~ outputs are requested to assign copyright to IEIP~~NIST~~ so that IEIP~~NIST~~ can cause them to be broadly licensed pursuant to a creative commons or similar license arrangement [NOTE: Identify appropriate open public licensing arrangement to cross reference and apply here]~~may place them in the public domain~~.

Standards developers whose standards are referenced in ~~SGIP~~IEIP outputs retain copyright ownership and control of the standards themselves.

***2.7 Ratification of the Bylaws and Amendments***

a. The ~~SGIP~~IEIP will have power to make, alter, amend, and repeal the Bylaws of the ~~SGIP~~IEIP by a vote of the ~~SGIP~~IEIP Participating Members. Approved amendments are effective immediately without any notice period

~~a. Any amendments and alterations that involve either NIST's role or the Administrator's role will require NIST concurrence.~~

~~c.~~b. For the initial ~~SGIP~~IEIP, Participating Members will ratify the Bylaws.

### ~~2.8~~1.7 *Conflict of Interest*

Members commit to seek~~are~~ to anticipate any situation in which a conflict of interest may arise and bring these concerns before the ~~SGIPGB~~IEIPGB and the Administrator for resolution. Resolution may involve the participating, observing, or governing board members of an organization with the conflict of interest recusing themselves from discussions and voting on a specific conflicting topic.

The perception by others of a conflict of interest can be as problematic as any formal legal impropriety. ~~SGIP~~IEIP and the ~~SGIPGB~~IEIPGB members must be sensitive to conflict of interest issues; however, being a Member of the ~~SGIP~~IEIP or the ~~SGIPGB~~IEIPGB should not disadvantage an individual or their affiliated organizations.

Members may present arguments and/or evidence of a conflict of interest to the ~~SGIPGB~~IEIPGB and the Administrator.

If a Member Voting Representative has a conflict and the Member Organization does not, the Member Organization may designate a different Voting Representative for the purpose of that vote or discussion.

### ~~2.9~~1.8 *Competition*

Recognizing that the membership of the ~~SGIP~~IEIP includes many business organizations that compete directly with one another, normal considerations of appropriate legal boundaries, including antitrust, where appropriate, will be observed. Inappropriate activities may include:

- discussion or engagement in fixing of product prices, allocation of customers or division of market
- discussion of status or substance of ongoing or threatened litigation.

### ~~2.10~~1.9 *Robert's Rules of Order*

All questions of parliamentary procedure not addressed in this Charter will be resolved according to Robert's Rules of Order Newly Revised (10th edition).[3] The Plenary Chair may select a Parliamentarian to interpret procedural rules and advise the Chair on procedural issues; the Plenary Secretary may fill this responsibility. Likewise, the ~~SGIPGB~~IEIPGB Chair will select a Parliamentarian to interpret procedural rules and advise the ~~SGIPGB~~IEIPGB Chair on procedural issues.

[3] *Robert's Rules of Order Newly Revised*, 10th edition, Perseus Books Group, Cambridge MA, 2000.

### ~~2.11~~1.10 *Offices*

The principal office of the ~~SGIP~~IEIP will be located at office of the Administrator. The ~~SGIP~~IEIP may have such other offices as the ~~Smart Grid~~Identity Ecosystem Interoperability Panel (~~SGIP~~IEIP) may designate or as the business of the ~~SGIP~~IEIP may require from time to time.

### ~~2.12~~1.11 *Charter Ratification*

For the initial ~~SGIP~~IEIP, Participating Members will ratify the Charter by simple majority vote.

Amendment of Charter: Amendment of the Charter may be accomplished only by a vote of the full ~~SGIP~~IEIP. Amendments to the Charter must be proposed and accepted using the following procedures:

a. Publication of a proposed amendment to the ~~SGIP~~IEIP Charter to Members by email and posting to the ~~SGIP~~IEIP Web site at least thirty (30) calendar days prior to the date of a ~~SGIP~~IEIP meeting or electronic vote;

b. Review by the ~~SGIPGB~~IEIPGB with a recommendation to the ~~SGIP~~IEIP endorsing or opposing the Charter amendment; and

c. An electronic vote by the ~~SGIP~~IEIP at which voting by a majority of Participating Members is verified by the Plenary Chair. Approval of an amendment requires an affirmative vote of 75% of eligible Participating Members voting.

## CERTIFICATE OF ADOPTION

The undersigned, being the Secretary of ~~SGIP~~IEIP, hereby certifies that the foregoing are the Bylaws adopted by resolution of the ~~SGIPGB~~IEIPGB of the ~~SGIP~~IEIP as of _____, 20__ and amended as of _____, 20__.

_____, Secretary

## ~~3.2.~~ Acknowledgement

Funding for the Administrator of the ~~SGIP~~IEIP, including meeting arrangements, related research and analysis, as well as the ~~SGIP~~IEIP administration and facilitation staff is currently provided [NOTE: Insert reference to funding source here]. ~~by to EnerNex Corporation under a contract from the National Institute of Standards and Technology, United States Department of Commerce~~.

## ~~4.3.~~ Revision History

| Version | Date | Change | Change Author |
|---|---|---|---|
| 0.1 | 7/4/11~~9/8/2009~~ | Preliminary Discussion ~~First~~ Draft | sld~~Ewg~~ |
| 0.2 | ~~9/10/2009~~ | ~~Editing into one "Charter" document~~ | ~~afs~~ |
| 0.3 | ~~9/10/2009~~ | ~~Reformatted section organization~~ | ~~Mjb~~ |
| 0.4 | ~~9/14/2009~~ | ~~Adjusted to standard template~~ | ~~Mjb~~ |
| 0.5 | ~~9/15/2009~~ | ~~Consistency edits~~ | ~~Mjb~~ |
| 0.6 | ~~9/16/2009~~ | ~~Merged in suggested edits from EG and GG~~ | ~~Mjb~~ |
| 1.0 | ~~9/17/2009~~ | ~~Final cleanup and edits~~ | ~~mjb~~ |
| ~~1.0b~~ | ~~9/28/2009~~ | ~~NIST comments~~ | ~~Vrs~~ |
| ~~1.0c~~ | ~~10/05/2009~~ | ~~Merge Documents and incorporate comments~~ | ~~mb/mt/kc~~ |
| ~~1.0d~~ | ~~10/10/2009~~ | ~~NIST comments and revisions~~ | ~~pab~~ |
| ~~1.0e~~ | ~~10/14/2009~~ | ~~EnerNex comments to NIST revisions~~ | ~~mt/kc~~ |
| ~~1.0f~~ | ~~10/15/09~~ | ~~EnerNex response to public comments~~ | ~~mb/mt/kc~~ |
| ~~1.0g~~ | ~~11/07/09~~ | ~~NIST comments and revisions~~ | ~~pab~~ |
| ~~1.0h~~ | ~~11/09/09~~ | ~~Additional NIST comments and revisions~~ | ~~pab/gwa~~ |
| ~~1.0i~~ | ~~11/11/09~~ | ~~Additional NIST comments and revisions~~ | ~~pab/gwa/mjl/al/dgh~~ |
| ~~1.0j~~ | ~~11/12/09~~ | ~~Additional NIST and EnerNex comments and revisions~~ | ~~pab/gwa/mjl/dp/mt/dh/mb~~ |
| ~~1.0k~~ | ~~11/13/09~~ | ~~Added ® to GridWise; correct version date stamp for 1.0f;~~<br><br>~~In order to clarify voting:~~<br><br>~~removed redundant voting description from membership section (2.2.1a,c) in favor of correct text in voting section (2.2.1.1.5); removed redundant description of voting (1.4.3); added reference in section 2.1.7.6 to GB election process from (2.2.1.1.5);~~ | ~~pab/mjb~~ |
| ~~1.01~~ | ~~11/14/09~~ | ~~Additional MST modifications for clarification. Revision of sections 2.6 and 2.7~~ | ~~Pab~~ |

| Version | Date | Change | Change Author |
|---|---|---|---|
| 1.1 | 3/25/2010 | Incorporated bylaws changes approved by SGIP Plenary on March 17, 2010 & editorial changes to Page iii, 2.2.6.1.3, 2.2.7, 2.4.1, and 2.6.1. | mt |
| 1.1a | 5/5/2010 | Restored 2.1.7.2 and 2.5.4 to version 1.01 wording. | |
| 1.2 | 6/10/10 | Incorporated bylaws changes approved by SGIP Plenary on May 25, 2010, involving 2.3.1, 2.3.2, 2.4 and 2.6. | mt |
| 1.3 | 6/10/11 | Incorporated bylaw changes approved by the SGIP Plenary on May 31, 2011, involving 2.1.1.1.i, 2.1.5, 2.3 and Appendix C. | mt |

## 5.4. References

This document makes use of the following references:


[1] ANSI™, 2009 ANSI Essential Requirements: Due process requirements for American National Standards

[2] National Strategy for Trusted Identities in Cyberspace, signed by the President on April 15, 2011"Energy Independence and Security Act of 2007", http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf

[3] GridWise™ Architecture Council Mission & Structure, December 2007, http://www.gridwiseac.org/pdfs/gwac_mission_structure.pdf

[4] GridWise™ Architecture Council Bylaws: 4 October 2004, http://www.gridwiseac,org.pdfs.gridwise_ac_bylaws.pdf

[5] HITSP Charter; ANSI Document Number: HITSP 06 N 109

[6] IEEE™ Charter and Bylaws Documents

[7] Internet Architecture Board; Charter of the Internet Architecture Board (IAB), RFC2850, May 2000

[8] NIST Smart Grid Conceptual Model, http://collaborate.nist.gov/twikisggrid/bin/view/SmartGrid/SGConceptualModel

[9] UCA™ International Users Group (UCAIug) Charter; UCAInternationalCharterRev3.1 Oct05

[10] UCA™ International Users Group (UCAIug) Bylaws; UCAInternationalBylawsRev2Oct2005

## APPENDIX A

## STAKEHOLDER CATEGORIES

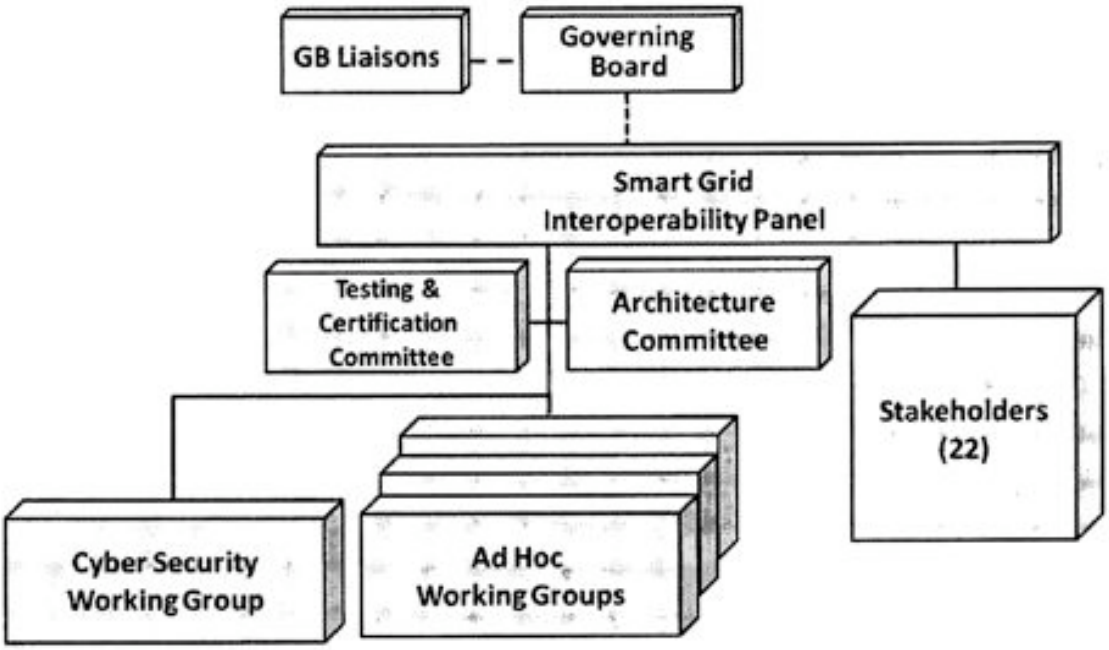
The following list is the list of Stakeholder Categories:

[to come]

1. Appliance and consumer electronics providers
2. Commercial and Industrial equipment manufacturers and automation vendors
3. Consumers - Residential, Commercial, and Industrial
4. Electric transportation industry Stakeholders
5. Electric utility companies – Investor Owned Utilities (IOU) and Publicly Owned Utilities
6. Electric utility companies - Municipal (MUNI)
7. Electric utility companies - Rural Electric Association(REA)
8. Electricity and financial market traders (includes aggregators)
9. Independent power producers
10. Information and communication technologies (ICT) Infrastructure and Service Providers
11. Information technology (IT) application developers and integrators
12. Power equipment manufacturers and vendors
13. Professional societies, users groups, trade associations and industry consortia
14. R&D organizations and academia
15. Relevant Federal Government Agencies
16. Renewable Power Producers
17. Retail Service Providers
18. Standard and specification development organizations (SDOs)
19. State and local regulators
20. Testing and Certification Vendors
21. Transmission operators and independent system operators
22. Venture Capital

**APPENDIX B**

**ORG CHART**



## APPENDIX C

## ACRONYMS

[NOTE: fill in this table as drafting proceeds]

| | |
|---|---|
| C&I | Commercial and Industrial |
| CTG | Coordination Task Group |
| DEWG | Domain Expert Working Group |
| DOC | Department of Commerce |
| ~~DOE~~ | ~~Department of Energy~~ |
| ~~EISA~~ | ~~Energy Independence and Security Act~~ |
| ICT | Information and Communication Technologies |
| IKB | Interoperability Knowledge Base |
| ~~IOU~~ | ~~Investor Owned Utilities~~ |
| IT | Information Technology |
| ~~MUNI~~ | ~~Municipal Utility~~ |
| NCSGI | National Coordinator for ~~Smart Grid~~Identity Ecosystem Interoperability |
| NIST | National Institute of Standards and Technology |
| PAP | Priority Action Plan |
| R&D | Research and Development |
| ~~REA~~ | ~~Rural Electric Association~~ |
| SDO | Standards Development Organization |
| ~~SGIP~~IEIP | ~~Smart Grid~~Identity Ecosystem Interoperability Panel |
| ~~SGAC~~IEAC | ~~Smart Grid~~Identity Ecosystem Architecture Committee |
| ~~SGCSWG~~IECSWG | ~~Smart Grid~~Identity Ecosystem Cyber Security Working Group |
| ~~SGIPGB~~IEIPG | ~~Smart Grid~~Identity Ecosystem Interoperability Panel Governing Board |

| | |
|---|---|
| B | |
| ~~SGTCC~~IETCC | ~~Smart Grid~~Identity Ecosystem Testing and Certification Committee |

**Exhibit 1.2.1A**

**Disclosure and Marking Practices for Identity Ecosystem Framework specifications**

Including standards for

normative and informative references to proprietary standards

and

those standards with respect to which various

intellectual property or other rights might be asserted

[to come]