



# **RECOMMENDATIONS FOR ESTABLISHING AN IDENTITY ECOSYSTEM GOVERNANCE STRUCTURE**

---

**THE DEPARTMENT OF COMMERCE  
NATIONAL INSTITUTE OF STANDARDS AND  
TECHNOLOGY**

Recommendations for Establishing an Identity  
Ecosystem Governance Structure

This page is intentionally left blank.

## Foreword

The Internet is one of the most transformative creations of modern history. It has shifted the way we, as individuals, organizations, nations, and businesses interact socially, economically, and intellectually. It is hard to find an aspect of society that has not in some way been impacted by the development of the Internet. Its reach spans across geographic, social, and economic borders and has created vast opportunities for the stimulation of commerce, innovation, and progress.

However, since the creation of the Internet, there have always been difficult questions surrounding privacy, security, and trust. How do we know with whom we are interacting? How do we know they are trustworthy? How do we balance the desires for anonymity and personal privacy with the need to secure our information and transactions? In an effort to address these questions, President Obama signed the *National Strategy for Trusted Identities in Cyberspace (NSTIC or “Strategy”)*.

The Strategy calls for the creation of an “Identity Ecosystem” – an online environment where individuals and organizations will be able to better trust each other because they follow agreed upon standards to obtain and authenticate their digital identities in a way that protects personal privacy, and also supports innovation and growth. By choosing to participate in this Identity Ecosystem, consumers and service providers alike would be confident in the identities of those institutions and individuals with whom they choose to interact, and in the security of their own private information.

Published in April of last year, NSTIC directed the Department of Commerce to establish a National Program Office (NPO) to coordinate the processes and activities necessary to implement the Strategy. While NIST was designated as the lead within the Department to establish the NPO, the NSTIC made clear that the private sector would be charged with building and operating the Identity Ecosystem. Among the foundational activities prescribed by the NSTIC was the establishment of a privately-led Steering Group to tackle the complex policy and technical issues necessary to create a framework for the Identity Ecosystem.

As the first step in the process, the NPO has produced this report which outlines the recommendations for the Identity Ecosystem Steering Group. As the lead organization for this interagency initiative, the NSTIC NPO has been able to call upon the experiences and talents of a diverse team of identity management, privacy and policy experts from across the government. Additionally, through a process of outreach workshops and a Notice of Inquiry, the NPO was able to reach out to private sector thought leaders and the general public. This report is the distillation of these inputs into recommendations for a private sector-led governance framework which remains faithful to the Strategy’s Guiding Principles while simultaneously promoting the innovation and participation that will be essential to making the Identity Ecosystem and the Strategy a success.

I would like to thank the respondents to the *Identity Ecosystem Governance Model Notice of Inquiry* and the many participants, both from industry and government, who attended our outreach meetings and workshops. Stakeholder participation is the key to the success of the NSTIC, and your efforts to this point have catalyzed significant and rapid forward progress. However, this report represents just an

Recommendations for Establishing an Identity  
Ecosystem Governance Structure

initial step towards the ultimate goal of an “Identity Ecosystem” that leads to unparalleled privacy, security, and prosperity on the Internet. We need your continued contributions to achieve success.

Sincerely,

Patrick Gallagher

Under Secretary of Commerce for Standards and Technology

Director, National Institute of Standards and Technology

## Executive Summary

The National Strategy for Trusted Identities in Cyberspace (NSTIC), signed by the President in April 2011, states, “A secure cyberspace is critical to our prosperity.” This powerful declaration makes clear that securing cyberspace is absolutely essential to increasing the security and privacy of transactions conducted over the Internet. The Identity Ecosystem envisioned in the NSTIC is an online environment that will enable people to validate their identities securely, but with minimized disclosure of personal information when they are conducting transactions. The vibrant marketplace created by the Identity Ecosystem will provide individuals with choices among multiple accredited identity providers, both private and public, and choices among multiple credentials. The added convenience, security, and privacy provided within the Identity Ecosystem will allow additional services to be put online to drive greater economic growth.

A core tenet of the NSTIC is that its implementation must be led by the private sector. The NSTIC calls for the Federal Government to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the processes by which online transactions are conducted. The Strategy itself was developed with substantial input from both the private sector and the American public. The National Institute of Standards and Technology (NIST), which has been designated to establish a National Program Office to lead the implementation of the NSTIC, recognizes that a continued public-private partnership is necessary for the execution of the Strategy’s vision across the wide range of interactions that occur over the Internet. As such, we are leading the effort to fulfill the NSTIC’s call for government to work in close partnership with the private sector and other relevant stakeholder groups, to, “[Establish a steering group to] administer the process for policy and standards development for the Identity Ecosystem Framework in accordance with the Guiding Principles in [the] Strategy.”

On June 8, 2011, a Notice of Inquiry (NOI) was published to solicit feedback and examples from the public regarding the establishment and structure of a private sector-led steering group. The release of the NOI was followed with a two-day public workshop in Washington, DC on June 9-10, 2011 where more than 270 people participated in a series of sessions on these four topics. This workshop provided an opportunity for participants to ask questions and engage in discussion in preparation for responding to the NOI. The NOI received 57 responses from a wide variety of stakeholders, including those from private industry, consumer advocacy and privacy organizations, state governments, and the financial and healthcare communities.

This report summarizes the responses to the NOI and provides recommendations and intended government actions to serve as a catalyst for establishing the Identity Ecosystem Steering Group (Steering Group). The recommendations are based on comments and suggestions from NOI respondents, best practices and lessons learned from similarly scoped governance efforts, and the Strategy itself. Our recommendations are not intended to be prescriptive, but rather are designed to facilitate the establishment of a vibrant and effective Steering Group within the private sector in accordance with the objectives set forth in NSTIC.

Key recommendations from the four topic areas are summarized below:

**Steering Group Initiation.** The Identity Ecosystem Steering Group should be established as a new organization which should be led by the private sector in conjunction with, but independent of the Federal Government. As a key stakeholder and active participant in the Identity Ecosystem, the government intends to catalyze the creation of this new governing body by funding, through a competitive grant, a service to provide secretarial (administrative and operational) support for the

Identity Ecosystem Steering Group. This Secretariat will also be charged with convening the initial meetings of the group and maintaining open and transparent operations. After a period of initial Government support, the Steering Group will need to establish a self-sustaining structure capable of allowing continued growth and operational independence. (Section 2.1)

**Steering Group Structure.** The government recommends a Steering Group structure with two bodies, a Plenary and a Management Council, with mutually supporting roles and dispersed decision making responsibilities. The Identity Ecosystem Plenary should be a large body containing working groups and committees dedicated to conducting the work required for establishing and adopting standards, policies, and procedures to govern the Identity Ecosystem. The Identity Ecosystem Management Council should be a smaller group consisting of officers, delegates from stakeholder groups, and at-large delegates. This council should be responsible for providing strategic guidance to the Plenary, supervising its progress, and resourcing its operations. Both of these structures, their officers, members, and staff should always operate according to the principles of openness, transparency, consensus, and harmonization and should always adhere to the NSTIC Guiding Principles. (Sections 2.2, 2.2.1, and 2.2.2)

**Stakeholder Representation.** Providing balanced representation, securing individual privacy, advocating for underrepresented participants, and preventing the exercise of undue influence are all essential aspects of providing effective stakeholder representation to participants in the Identity Ecosystem. For this reason, this report describes multiple safeguards that are designed to work in concert to provide protections for individual privacy and the underrepresented, and guard against undue influence by any one stakeholder group. Some of the safeguards called for throughout this report are:

- **A Privacy Coordination Committee** - A permanent body responsible for reviewing and approving all Steering Group standards, policy, and procedures to ensure they do not violate accepted privacy standards. (Sections 2.2.1 and 2.3)
- **An Ombudsman** - An impartial and unaffiliated officer responsible for supporting equitable representation of all stakeholders and individual participants and upholding the Guiding Principles. (Sections 2.2.2 and 2.3)
- **Operating Principles** - All operations within the Steering Group should be conducted in accordance with the principles of openness and transparency, balance, consensus, and harmonization. (Sections 2.2.1, 2.2.2, and 2.3)
- **One Member, One Vote** - Within the Plenary and on the Management Council no single stakeholder group or organization should have more than one vote in decision making proceedings. (Sections 2.2.1, 2.2.2, and 2.3)
- **Multiple Pathways to Participation** - The Identity Ecosystem Steering Group should maintain multiple pathways to allow all stakeholders the broadest opportunity to take part – directly or indirectly – in the Steering Group. (Section 2.3)

**International Coordination.** Given the global nature of online commerce, the Identity Ecosystem cannot be isolated from internationally available online services and their identity solutions. As such, the Identity Ecosystem Steering Group should coordinate with representatives from ongoing and planned international identity efforts, standards development organizations, trade organizations, and the international departments of member entities in order to leverage lessons learned and broadly recognized technical standards. Additionally, the Steering Group should promote international participation and where appropriate, should strive to identify and use internationally recognized policies and standards that meet applicable assessment criteria and conform to the NSTIC Guiding Principles. (Section 2.4)

Recommendations for Establishing an Identity  
Ecosystem Governance Structure

The NSTIC National Program Office is committed to the Strategy and to fostering the development of the Identity Ecosystem and this report is intended to serve as the initial step in stimulating the creation of an effective governance structure. Additionally, we are including a recommended Charter to help streamline the effort to formally establish the Steering Group. These documents are intended to provide a starting point from which the Identity Ecosystem can expand and evolve.

## Table of Contents

<b>Foreword</b>	<b>iii</b>
<b>Executive Summary</b> .....	<b>v</b>
<b>Table of Contents</b>	<b>viii</b>
<b>1. Introduction</b>	<b>1</b>
1.1. The Identity Ecosystem .....	2
1.2. Notice of Inquiry: Models for a Governance Structure for the NSTIC .....	5
<b>2. Recommendations for the Identity Ecosystem Steering Group</b> .....	<b>6</b>
2.1. Steering Group Initiation .....	6
2.2. Steering Group Structure .....	9
2.3. Stakeholder Representation .....	19
2.4. International Coordination .....	24
2.5. Recommended Steering Group Charter .....	25
<b>3. The Road Ahead</b> .....	<b>26</b>
<b>Appendix A – Steering Group Recommendations Summary</b> .....	<b>27</b>
<b>Appendix B – Recommended Identity Ecosystem Steering Group Charter</b> .....	<b>31</b>
<b>1. Identity Ecosystem Steering Group Charter</b> .....	<b>1</b>
1.1. Mission .....	2
1.2. Scope of Activities .....	2
1.3. Adherence to the NSTIC Guiding Principles .....	3
1.4. Operating Principles .....	4
1.5. Membership .....	5
1.6. Organizational Structure .....	5
1.7. Establishment .....	5
<b>2. Identity Ecosystem Plenary</b> .....	<b>7</b>
<b>3. Identity Ecosystem Management Council</b> .....	<b>9</b>
3.1. Management Council Composition .....	9
3.2. Management Council Selection .....	9
<b>4. Secretariat</b>	<b>12</b>



## 1. Introduction

The National Strategy for Trusted Identities in Cyberspace (NSTIC or Strategy), signed by President Obama in April 2011, acknowledges and addresses a major weakness in cyberspace – a lack of confidence and assurance that people, organizations, and businesses are who they say they are online.<sup>1</sup> Additionally, in the current online environment, individuals are asked to maintain dozens of different usernames and passwords, one for each website with which they interact. The complexity of this approach is a burden to individuals, and it encourages behavior – such as the reuse of passwords – that makes online fraud and identity theft easier. At the same time, online businesses are faced with ever-increasing costs for managing customer accounts, the consequences of online fraud, and the loss of business that results from individuals’ unwillingness to create yet another account. Moreover, both businesses and governments are unable to offer many services online, because they cannot effectively identify the individuals with whom they interact. Spoofed websites, stolen passwords, and compromised accounts are all symptoms of inadequate authentication mechanisms.<sup>2</sup>

The Identity Ecosystem envisioned in the NSTIC is an online environment that will enable people to validate their identities securely, but with minimized disclosure of personal information when they are conducting transactions. The vibrant marketplace created by the Identity Ecosystem will provide people with choices among multiple accredited identity providers, both private and public, and choices among multiple credentials. For example, imagine that a student could get a digital credential from her cell phone provider and another one from her university and use either of them to log-in to her bank’s website, her e-mail, three social networking sites, four online commerce sites, and so on, all without having to remember dozens of passwords. The added convenience, security, and privacy provided within the Identity Ecosystem will allow additional services to be put online to drive greater economic growth. Notwithstanding the objective to improve identification and authentication in cyberspace for certain types of transactions, not all Internet activities have such needs. Thus, the capacity for anonymity and pseudonymity will be maintained in the envisioned Identity Ecosystem.

A core tenet of the NSTIC is that its implementation must be led by the private sector. The NSTIC calls for the Federal Government to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the processes by which online transactions are conducted. The Strategy itself was developed with substantial input from both the private sector and the American public. The National Institute of Standards and Technology (NIST), which has been designated to establish a National Program Office to lead the implementation of the NSTIC, recognizes that a strong and vibrant public-private partnership is necessary to execute the Strategy’s vision in a way that supports the wide range of interactions that occur over the Internet. As such, NIST is leading the effort to fulfill the NSTIC’s call for government to work in close partnership with the private sector and other relevant stakeholder groups to, “[Establish a steering group to] administer the process for policy and standards development for the Identity Ecosystem Framework in accordance with the Guiding Principles in

---

<sup>1</sup> The full Strategy can be found at: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/NSTICstrategy\\_041511.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf)

<sup>2</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, 1.

[the] Strategy. The steering group will also ensure that accreditation authorities validate participants' adherence to the requirements of the Identity Ecosystem Framework.”<sup>3</sup>

On June 14, 2011, a Notice of Inquiry (NOI) was published in the *Federal Register* to solicit feedback and examples from the public regarding the establishment and structure of a private sector-led steering group.<sup>4</sup> A second notice was published in the *Federal Register* on August 16, 2011, extending the comment period until August 30, 2011.<sup>5</sup> This report summarizes the responses to the NOI and provides recommendations and intended government actions to serve as a catalyst for establishing such a governance structure. The recommendations result from comments and suggestions by the NOI respondents as well as best practices and lessons learned from similarly scoped governance efforts. These Federal Government recommendations are not intended to be prescriptive, but rather are designed to facilitate the establishment of a vibrant and effective Identity Ecosystem Steering Group (Steering Group) within the private sector in accordance with the objectives set forth in NSTIC. To further accelerate the launch of the Steering Group, Appendix B integrates the recommendations into a proposed charter.

## 1.1. The Identity Ecosystem

The NSTIC specifies that, “The Identity Ecosystem will consist of different online communities that use interoperable technology, processes, and policies. These will be developed over time – but always with a baseline of privacy, interoperability, and security.”<sup>6</sup> This baseline will be provided by the Identity Ecosystem Framework, which is the overarching set of roles and responsibilities, interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that govern all of the individual online communities that comprise the Identity Ecosystem.<sup>7</sup> Each of the parties involved in the operation of the Identity Ecosystem – Identity Providers, Relying Parties, Attribute Providers, and Accreditation Authorities play a pivotal role in maintaining and complying with the Identity Ecosystem Framework as illustrated in Figure 1. Furthermore, these parties are all stakeholders in the Identity Ecosystem; their representation and involvement in the Steering Group is crucial to the overall success of the Ecosystem.

The bullets below define the various roles and responsibilities within the Identity Ecosystem as defined in the Strategy.<sup>8</sup>

- An **individual** is a person engaged in an online transaction. Individuals are the first priority of the Strategy.
- A **non-person entity (NPE)** may also require authentication in the Identity Ecosystem. NPEs can be organizations, hardware, networks, software, or services and are treated much like individuals within the Identity Ecosystem. NPEs may engage in or support a transaction.

---

<sup>3</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, p. 25.

<sup>4</sup> Federal Register, Vol. 76, No. 114 (June 14, 2011): pp. 34650-34653.

<sup>5</sup> Federal Register, Vol. 76, No. 158 (August 16, 2011): p. 50719.

<sup>6</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, p. 24.

<sup>7</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, p. 24.

<sup>8</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, pp. 21-22, 25.

- The **subject** of a transaction may be an individual or a non-person entity (i.e., organizations, hardware, networks, software, or services that are treated much like individuals in a transaction).
- An **identity provider** is responsible for establishing, maintaining, and securing the digital identity associated with a subject. These processes include revoking, suspending, and restoring the subject's digital identity if necessary.
- A **relying party** makes transaction decisions based upon its receipt, validation, and acceptance of a subject's authenticated credentials and attributes. Within the Identity Ecosystem, a relying party selects and trusts the identity and attribute providers of their choice, based on risk and functional requirements.
- An **attribute provider** is responsible for the processes associated with establishing and maintaining identity attributes. Attribute maintenance includes validating, updating, and revoking the attribute claim. An attribute provider asserts trusted, validated attribute claims in response to attribute requests from relying parties.
- **Participants** refer to the collective subjects, identity providers, attribute providers, relying parties, and identity media taking part in a given transaction.
- An **accreditation authority** assesses and validates identity providers, attribute providers, relying parties, and identity media, ensuring that they all adhere to an agreed-upon trust framework. Accreditation authorities can issue trustmarks to the participants that they validate.
- A **trust framework** is developed by a community whose members have similar goals and perspectives. It defines the rights and responsibilities of that community's participants in the Identity Ecosystem; specifies the policies and standards specific to the community; and defines the community-specific processes and procedures that provide assurance. A trust framework considers the level of risk associated with the transaction types of its participants; for example, for regulated industries, it could incorporate the requirements particular to that industry. In order to be a part of the Identity Ecosystem, all trust frameworks must still meet the baseline requirements established by the Identity Ecosystem Framework.

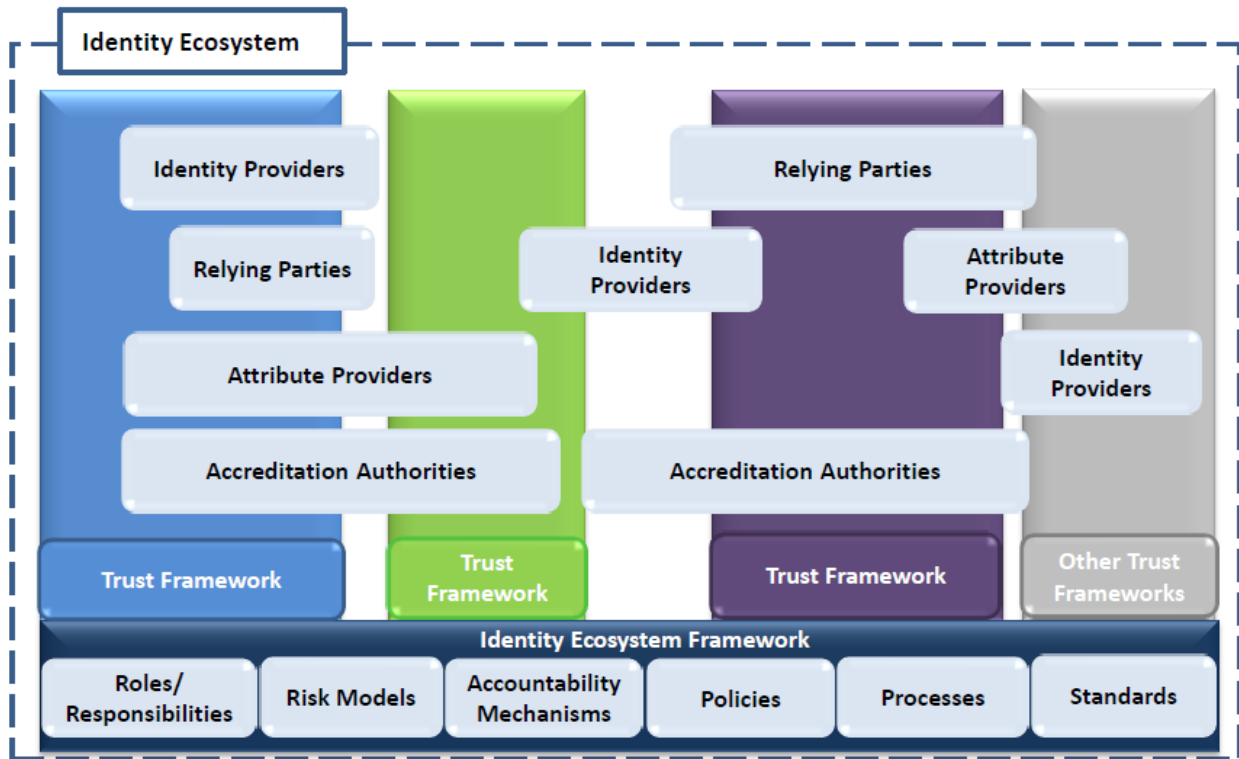


Figure 1: NSTIC Vision of the Identity Ecosystem

As depicted in Figure 1, the Identity Ecosystem (“Ecosystem”) is made up of many individual trust frameworks that have all been accredited to comply with a baseline set of requirements (the “Identity Ecosystem Framework” or “Framework”) for operating within the Ecosystem. The parties shown (identity providers, attribute providers, relying parties, and accreditation authorities) may serve multiple, and perhaps overlapping, trust frameworks within the Ecosystem. The Framework, however, establishes a uniform trust that all of the parties and trust frameworks with whom they may interact online meet established requirements.

### **The Steering Group**

The establishment of a privately-led governance structure to administer the process for standards adoption, accreditation, and policy development is a foundational step toward implementation of the Identity Ecosystem and achievement of the NSTIC vision. The Steering Group is primarily responsible for supporting the achievement of the goals outlined in the Strategy and fostering the establishment of the Identity Ecosystem Framework. In its operations, the Steering Group must be guided by and uphold the four NSTIC Guiding Principles:<sup>9</sup>

- Identity solutions will be privacy-enhancing and voluntary;
- Identity solutions will be secure and resilient;
- Identity solutions will be interoperable; and
- Identity solutions will be cost-effective and easy to use.

<sup>9</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, 11.

The purpose and role of the Steering Group is outlined in the Strategy under Objective 1.4:

The policy and technical standards necessary for the Identity Ecosystem may be developed in different forms. A steering group will thus administer the process for policy and technical standards development for the Identity Ecosystem Framework. The group will bring together all of the interested stakeholders to ensure that the Identity Ecosystem Framework provides a minimum baseline of privacy, security, and interoperability through standards, policies, and laws—without creating unnecessary barriers to entry. The steering group will work diligently to follow the Guiding Principles in this Strategy; it will organize and conduct itself in the spirit of those principles, as the inclusive, transparent, pragmatic, and committed leadership group building toward the Strategy’s vision. To that end, the steering group will also set milestones and measure progress. The steering group will also ensure that accreditation authorities validate participants’ adherence to the requirements of the Identity Ecosystem Framework.<sup>10</sup>

## **1.2. Notice of Inquiry: Models for a Governance Structure for the NSTIC**

The NOI solicited input in on the key issues associated with creating a Steering Group to develop the Identity Ecosystem Framework, organized around four specific areas – Structure of the Steering Group, Steering Group Initiation, Representation of Stakeholders within the Steering Group, and International Coordination.

In addition, NIST held a two-day public workshop in Washington, DC on June 9-10, 2011 where more than 270 people participated in a series of sessions on these four topics. This workshop provided an opportunity for participants to ask questions and engage in discussion in preparation for responding to the NOI. The NOI received 57 responses from a wide variety of stakeholders, including those from private industry, consumer advocacy and privacy organizations, state governments, and the financial and healthcare communities. These responses are publicly available on the NSTIC Website at: <http://www.nist.gov/nstic/governance-comments.html>.

---

<sup>10</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, 31.

## 2. Recommendations for the Identity Ecosystem Steering Group

This report consists of five subsections. The first four subsections summarize relevant points from the NOI responses and outlines recommendations for addressing the core challenges associated with standing up the Steering Group. The final subsection is a recommended charter for the Steering Group.

- Steering Group Initiation
- Steering Group Structure
- Stakeholder Representation
- International Coordination
- Recommended Steering Group Charter

### 2.1. Steering Group Initiation

#### Organization

In accordance with the Strategy, the government's role is to facilitate and accelerate establishment of the Steering Group. The NOI asked a wide range of questions related to initiation of the Steering Group. In particular, it delineated several means by which the Steering Group could be established including: as an entirely new organization, an element of an existing organization, or through a government authority, such as a formally chartered Federal Advisory Committee which falls under the Federal Advisory Committee Act (FACA).<sup>11</sup>

NOI responses varied significantly on the question of whether the Identity Ecosystem should be governed by an existing organization or whether an entirely new structure should be established as the Steering Group. Of note, however, no existing organization was identified by the respondents as having the breadth of stakeholder membership and diversity of focus and experience necessary to govern the Identity Ecosystem.

A number of the NOI respondents were opposed to the creation of a Federal Advisory Committee, arguing that the FACA statute should not apply.<sup>12</sup> A common theme was that the Steering Group, as envisioned by the NSTIC, would not have the mission of providing the Government with advice or recommendations (the kinds of activities called out under FACA). Rather, the Steering Group would be tasked to lead the activities needed to establish and govern the Identity Ecosystem. The NSTIC states, "Only the private sector has the ability to build and operate the complete Identity Ecosystem, and the final success of the Strategy depends upon private-sector leadership and innovation."<sup>13</sup> NSTIC envisions that government will be one of many stakeholders at the table in the Steering Group; however, as this paper details, government will not actually be making decisions for the Group. That power will rest within the membership of the Steering Group itself.

---

<sup>11</sup> Federal Register, Vol. 76, No. 114 (June 14, 2011): p. 34652.

<sup>12</sup> See, e.g., U.S. Chamber of Commerce at 2.4, CertiPath at 7, and Microsoft at 7, Response to NIST NOI.

<sup>13</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, p. 37.

Among the 57 responses, only one advocated for the Steering Group to be a Federal Advisory Committee. Of note the respondent favored this course in part because of several important statutory “rights and obligations that are imposed by FACA,”<sup>14</sup> such as requirements for transparent administrative procedures and open meetings.

We agree that the Steering Group must be operational, not merely advisory; therefore a Federal Advisory Committee is not the right model for the Steering Group. Nonetheless, we consider operational aspects of Federal Advisory Committees such as transparent procedures and open meetings to be key elements for achieving an effective Steering Group. These elements are addressed in more detail in section 2.3 as well as the Recommended Charter (Appendix B).

The Federal Government currently has a statutory advisory committee established in accordance with the FACA, the Information Security and Privacy Advisory Board (ISPAB), that provides advice and recommendations on a wide range of issues associated with digital identity and privacy.<sup>15</sup> The NSTIC Program Director meets with them on a quarterly basis. For any areas where the Federal Government is seeking advice or recommendations from the private sector on topics related to the Identity Ecosystem, it will continue to leverage the ISPAB.

**Recommendation 01:** Given the unique and complex nature of the Identity Ecosystem and the role the NSTIC envisions the government playing in its formation, the Steering Group should be established as a new organization to be led by the private sector.

### **Government Support**

Recognizing the difficulty associated with establishing a Steering Group for the Identity Ecosystem, the NOI requested comment on “How can the government be most effective in accelerating the development and ultimate success of the Identity Ecosystem?”<sup>16</sup> Several NOI respondents suggested that the initiation of the Steering Group would require material, logistical, and financial support from the Federal Government in order to be successful.<sup>17</sup> This opinion was clearly expressed in one particular response which stated, “The objective of [the] NSTIC's initial phase should be to use government leverage to encourage a self-governance structure that weans itself off of the need for support.”<sup>18</sup> This respondent also pointed out that the creation of the Steering Group will require a high degree of communication with the disparate stakeholder groups that will participate in the Identity Ecosystem. Additional comments specified the need for an administrative body dedicated to supporting the operations of the entire Steering Group.<sup>19</sup> In order to meet the logistical and administrative demands of the Steering Group’s creation, NOI respondents proposed that initial

---

<sup>14</sup> The Electronic Privacy Information Center and The Liberty Coalition, Response to NIST NOI, p. 4.

<sup>15</sup> For more information on the ISPAB refer to: <http://csrc.nist.gov/groups/SMA/ispab/>

<sup>16</sup> Federal Register, Vol. 76, No. 114 (June 14, 2011): p. 34652.

<sup>17</sup> See, e.g., SAFE BioPharma at 10, Civics.com at 6, EDUCAUSE/Internet2/InCommon at 6, Electronic Frontier Foundation at 2-4, Kantara at 5, OASIS at 5-6, Open Identity Exchange at 39, 84-86, 90-94, Financial Services Sector Council for Critical Infrastructure Protection and Homeland Security at 3-4, Deloitte & Touche LLP at 3, vDesk at 6, IBM at 3, Verizon at 2, and Dutch Ministry of Economic Affairs, Agriculture and Innovation at 6-7, Responses to NIST NOI.

<sup>18</sup> OASIS, Response to NIST NOI, p. 6.

<sup>19</sup> See, e.g., The University of Texas Center for Identity at 3 and International Biometrics & Identification Association at 1, Response to NIST NOI.

government funding would be best used to secure an ongoing secretarial/administrative support role.<sup>20</sup>

Many NOI responses also expressed the desire for initial Federal oversight to ensure that privacy as well as stakeholder and individual representation were protected during the establishment and ongoing operations of the Steering Group.<sup>21</sup> A few feared that existing gaps in the size, financial resources, and objectives of the various Identity Ecosystem stakeholders could be exacerbated if they were not effectively mitigated during the creation process. They argued that the government, as a significant stakeholder in the Identity Ecosystem with a clear strategic interest in both privacy and balanced representation, would be best positioned to support the Steering Group in addressing these concerns early in its creation.

We agree that the government should play a significant role in catalyzing the initial formation of the Steering Group.

**Recommendation 02:** The government will accomplish this by funding, through a competitive grant, a secretariat service (the Secretariat) for the Steering Group.

**Recommendation 03:** The Secretariat will be charged with convening the initial meeting of the Steering Group, and providing administrative and logistical services and material support to the Steering Group (including the Working Groups and Standing Committees detailed in section 2.2.1) and maintaining openness and transparency in all Steering Group functions, all with an eye toward aligning the Steering Group's operations with the NSTIC Guiding Principles.

### **Funding**

In the NOI, we asked several questions with regard to long term funding for the ongoing operations of the Steering Group.<sup>22</sup> One NOI respondent stated that, “the Steering [Group] must create a sustainable funding model” and be capable of supporting ongoing operations, rather than being dependent on the Federal Government or another external source of funding.<sup>23</sup> Furthermore, multiple respondents cited the need for immediate development of a sustainable model in which the Steering Group derives its funding from the operation of the Identity Ecosystem while not impeding stakeholder participation or voting rights.<sup>24</sup> This foundational step could eliminate any future dependency on an external organization for funding and allow the Steering Group to become self-sustaining and accessible to all stakeholders.

---

<sup>20</sup> See, e.g., vDesk at 6, Dutch Ministry of Economic Affairs, Agriculture and Innovation at 6-7, and SAFE BioPharma at 10, Response to NIST NOI.

<sup>21</sup> See, e.g., Kantara at 9, Microsoft at 1-2, Open Identity Exchange at 83, Southern Michigan Health Information Exchange at notation 2.2, Timothy Jurgensen at 2, 5-6, 9, and Civics.com at 6, Response to NIST NOI.

<sup>22</sup> Federal Register, Vol. 76, No. 114 (June 14, 2011): p. 34653.

<sup>23</sup> Verizon, Response to NIST NOI, appendix A.

<sup>24</sup> See, e.g., Jericho Forum at 6, Online Trust Alliance at 2, Open Identity Exchange at 57, Smart Card Alliance at 1-3,6, and Verizon at 2, Response to NIST NOI.



Respondents' steady-state funding suggestions can be categorized into the following three potential sources. As part of its analysis the Steering Group should consider all viable self-sustaining funding models including, but not limited to:

- **Transaction-related fee.**<sup>25</sup> It is possible that a small fee or a percentage of monetary transactions conducted in the Identity Ecosystem could be levied to provide an ongoing and sustainable source of funding.
- **Role-holder accreditation fees.**<sup>26</sup> Certification and accreditation processes for the various role holders within the Identity Ecosystem (e.g., Identity Providers, Relying Parties, Credential Providers, and Attribute Providers) and corresponding use of the Identity Ecosystem Trustmark could have an associated fee that could be used to fund the governance and management of the Identity Ecosystem.
- **Tiered Membership Fee Structure.**<sup>27</sup> If deemed necessary, a series of fee levels for stakeholders based on established criteria (e.g., stakeholder type, size, role within the governance body, etc.) could be implemented to sustain operations of the Steering Group.

**Recommendation 04:** The Steering Group should conduct an analysis of potential self-sustaining funding models which should be implemented following a period of initial support from the Federal Government.

**Recommendation 05:** To support fair representation among stakeholders with varied resources, there should be no correlation between fees charged to Steering Group participants and the ability to vote or impact decision-making within the Steering Group.

## 2.2. Steering Group Structure

### Governance Model

In order to implement the Strategy, the Steering Group identified in Section 1.1 must establish a robust governance structure. This structure must be capable of addressing the need to create and adopt the policies, processes, and standards through which the Identity Ecosystem Framework will operate, while maintaining alignment with the NISTIC Guiding Principles. Part of its NOI requested input on existing “broad, multi-sector governance structures”<sup>28</sup> which may be used as models on which the Steering Group could be based. Although several organizational models were cited as potential examples that could be leveraged in constructing the Steering Group, the majority of responsive comments stated that the Identity Ecosystem should emulate the two-tiered organizational model of the Smart Grid Interoperability Panel (SGIP).<sup>29</sup>

---

<sup>25</sup> See, e.g., Dutch Ministry of Economic Affairs, Agriculture and Innovation at 8, Microsoft at 10, and Morpheus Technologies Inc at 1, Response to NIST NOI.

<sup>26</sup> See, e.g., vDesk at 7, Verizon at 2, appendix A, Open Identity Exchange at 112, Online Trust Alliance at 2 and CertiPath at 5, and U.S. Public Policy Council of the Association for Computing Machinery at 3, Response to NIST NOI.

<sup>27</sup> See, e.g., U.S. Public Policy Council of the Association for Computing Machinery 2, Open Identity Exchange at 113, Unisys at 4, Southern Michigan Health Information Exchange at notation in 3.4, Smart Card Alliance at 6, and Daon at 7, Response to NIST NOI.

<sup>28</sup> Federal Register, Vol. 76, No. 114 (June 14, 2011): p. 34652.

<sup>29</sup> See, e.g., OASIS at 1-7, Open Identity Exchange at 12, 28, appendix C, CertiPath at 6, Deloitte & Touch LLP at 8, Morpheus Technologies Inc. at 1, and The University of Texas Center for Identity at 11, Response to NIST NOI.

The SGIP contains a large open plenary with working groups and committees, a smaller governing council selected based upon stakeholder group alignment, and various officers to lead the governance structure.

As background, the SGIP was established in response to a growing need for interoperable technologies, standards, policies, and security practices in the electric and power industry. Its governance structure was developed to address complex issues of interoperability, stakeholder representation, and security very similar to those that face the Identity Ecosystem Steering Group. The government funded a secretariat service charged with both creating the SGIP and supporting its day to day operations.

While the SGIP was the example most recommended by NOI respondents, some of these respondents raised certain caveats about leveraging the SGIP as a model. For example, SGIP's purpose is limited to establishing interoperability, privacy, security, and usability across the electricity industry and related government stakeholders. In comparison, the Identity Ecosystem crosses virtually all industry sectors, includes an equally broad range of governmental stakeholders, and must take into account individual users as stakeholders. Accordingly, some respondents suggested that the SGIP structure, while ideally suited to the challenges faced by the electricity industry, must be modified and adapted to accommodate the unique characteristics and individual-centric nature of the Identity Ecosystem. One NOI respondent noted the SGIP as a good starting point, stating, "Smart Grid is a sector-specific, yet useful model...the organizational model is useful as a discussion starter."<sup>30</sup> Another respondent noted, "SGIP is focused on a [narrower] engineering problem...[and] may require...adaptation to make the SGIP model effective."<sup>31</sup> We agree that although certain elements of the SGIP organizational structure have proven to be an effective governance model, the role of individuals and the use of such sensitive information as identity attributes, in addition to the broad reach of the Identity Ecosystem, calls for additional mechanisms to achieve the objectives of the NSTIC Guiding Principles. Therefore, our recommendations propose a governance structure that leverages key attributes of the SGIP model, while also reflecting the unique challenges of the Identity Ecosystem.

The particular attribute of the SGIP that we believe is most compelling is its two-tiered structure, which has enabled the development of a broad representative base that incorporates a range of stakeholder groups with a depth of expertise. Additionally, the distribution of authority and decision-making responsibilities among the two tiers has prevented one segment, or stakeholder group, from establishing undue or excessive influence over the entire governance structure.

**Recommendation 06:** The Steering Group should be established as a two-tiered structure.

### **Governing Bodies**

One respondent suggested that one body comprise a large "public assembly"<sup>32</sup>, where various stakeholders of the Identity Ecosystem with diverse skill sets and interests could conduct the work necessary to develop policies and promote technical standards for the Identity Ecosystem

---

<sup>30</sup> CertiPath, Response to NIST NOI, p. 6.

<sup>31</sup> Educause/ Internet2/ InCommon, Response to NIST NOI, p. 4.

<sup>32</sup> Microsoft, Response to NIST NOI, p. 9.

Framework.<sup>33</sup> While there were varied responses as to exactly how this structure should work and what it should be composed of, most responsive comments agreed on a single significant point – the Plenary (referenced with a variety of different terms in the NOI responses) should be, “inclusive and accessible [of all stakeholder groups]” and “experienced and knowledge intensive [across all Identity Ecosystem knowledge areas].”<sup>34</sup>

**Recommendation 07:** The Identity Ecosystem Plenary should be established to review and recommend technical standards for adoption, establish and maintain the policies and procedures that govern the Identity Ecosystem, develop and establish accountability measures to promote broad adherence to these procedures, and facilitate the ongoing operation of the Steering Group.

**Recommendation 08:** The Plenary should be open to all stakeholders and individuals who wish to participate in the Identity Ecosystem Steering Group.

In addition to the Plenary, many NOI responses called for a smaller executive body to handle the organizational and oversight requirements of the Identity Ecosystem Steering Group.<sup>35</sup> One particular response detailed the need for an administrative or managing body to address sustainable operations requirements, set working goals, provide strategic guidance, and oversee the production of policy and standards.<sup>36</sup>

**Recommendation 09:** The Identity Ecosystem Management Council should be created to provide guidance to the Plenary on the broad perspectives envisioned by the Strategy: produce, prioritize and monitor progress of Steering Group work plans, and ensure that Steering Group work activities adhere to the NSTIC Guiding Principles and Goals; and ratify policy and standards recommendations approved by the Plenary. The Management Council should be responsible for managing the Steering Group’s resources and procuring services once the Steering Group is self-sustaining, as necessary.

**Recommendation 10:** Decision-making authority should be divided between the two groups, with the Plenary responsible for reviewing and approving standards and policies within its working groups and committees and the Management Council ratifying those standards and policies based on the recommendation of the Plenary. Implementation of this two-tiered approach allows for broad participation by all stakeholders and provides the added assurance of a focused executive layer (Management Council) to support the Steering Group with the resources and strategic direction necessary to accomplish its work. The recommended composition of the Plenary and Management Council are further discussed in Sections 2.2.1 and 2.2.2, respectively.

Figure 2 below provides a high-level illustration of the two-tier Steering Group structure.

---

<sup>33</sup> Daon, Response to NIST NOI, p. 4.

<sup>34</sup> The University of Texas Center for Identity, Response to NIST NOI, pp. 2-3.

<sup>35</sup> See, e.g., EDUCAUSE/Internet2/InCommon at 3-4, Open Identity Exchange at 27, 137-138, appendix C, Microsoft at 2, Peter F. Brown 1-7, Timothy Jurgensen at 10, Financial Services Sector Council for Critical Infrastructure Protection and Homeland Security at 2-3, and vDesk at 1-5, Response to NIST NOI.

<sup>36</sup> Smart Card Alliance, Response to NIST NOI, p. 2.

## RECOMMENDED IDENTITY ECOSYSTEM STEERING GROUP GOVERNANCE STRUCTURE

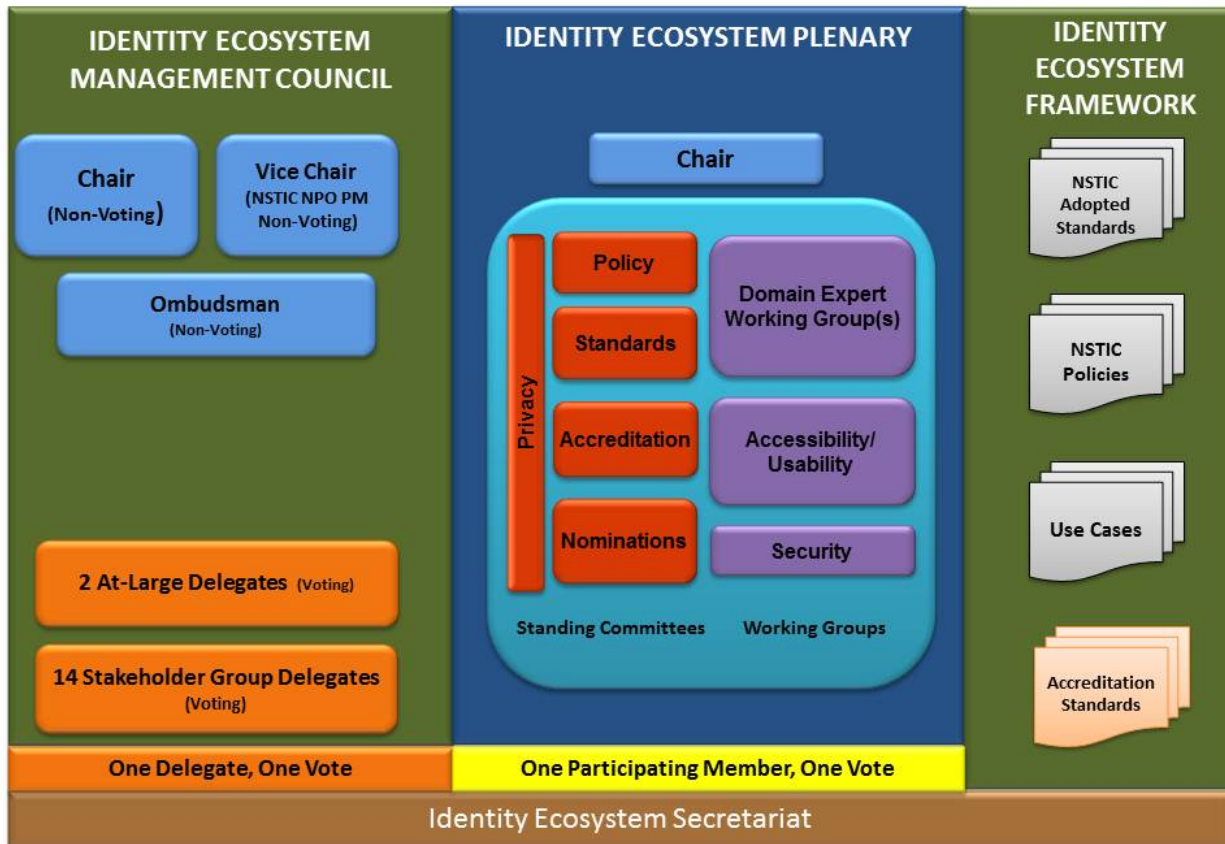


Figure 2: Recommended Identity Ecosystem Steering Group Structure

Table defines recommended key roles within the Identity Ecosystem Steering Group Structure. The sections where each item can be found in this report are included after each definition.

Table 1: Summary of Recommended Identity Ecosystem Steering Group Structure

Summary of Recommended Identity Ecosystem Steering Group Structure	
<b>Identity Ecosystem Plenary</b>	Reviews and recommends technical standards for adoption, establishes and maintains the procedures/policies for governing the Identity Ecosystem, develops and establishes accountability measures to promote broad adherence to these procedures, and facilitates the ongoing operation of the Steering Group. Open to all members of the Steering Group. (2.2.1)
<b>Identity Ecosystem Management Council (“Management Council”)</b>	Provides guidance to the Plenary on the broad objectives envisioned by the Strategy; produces, prioritizes and monitors progress of Steering Group work plans; provides necessary resources, and ensure that Steering Group work activities adhere to the NSTIC Guiding Principles and Goals; and ratifies policy and standards recommendations approved by the Plenary. (2.2.2)
<b>Working Groups</b>	Temporary/ad hoc groups established to conduct the work necessary for standards adoption and policy development/implementation as needed. (2.2.1)
<b>Standing Committees</b>	Committees created to coordinate ongoing and/or permanent activities that occur within the Plenary. (2.2.1)

<b>Summary of Recommended Identity Ecosystem Steering Group Structure</b>	
<b>Participating Member</b>	Those stakeholders who are able to commit the time and resources to attending the meetings and contributing to the work of the Plenary and its Standing Committees and Working Groups. Participating Members will be allowed to vote in the Plenary. (2.2.1)
<b>Observing Member</b>	Those stakeholders that do not make the commitment to actively participate but may attend meetings and review Plenary work products. Observing Members will not be permitted to vote in the Plenary. (2.2.1)
<b>Plenary Chair</b>	In the Plenary, this individual provides direction for actions, manages meetings, supervises votes/elections, and provides general leadership the Plenary. (2.2.1)
<b>Secretariat</b>	Provides administrative and material support to the Identity Ecosystem Steering Group. (2.1)
<b>Management Council Delegates</b>	Individuals elected to represent each of the 14 Stakeholder Groups on the Identity Ecosystem Management Council. There are an additional two at-large delegates. (2.2.2)
<b>Management Council Chair</b>	This individual provides general leadership to the Management Council; oversees votes, and directs the meetings of the Management Council. (2.2.2)
<b>Management Council Vice-Chair</b>	This individual serves in a capacity that guides the Steering Group toward successful implementation of the NSTIC and that it maintains alignment with the NSTIC Guiding Principles. It is recommended that this position be filled by the Director of the NSTIC NPO. (2.2.2)
<b>Ombudsman</b>	This position serves to support equitable representation of all stakeholders and individual participants in the Identity Ecosystem and upholds the NSTIC Guiding Principles. This position should be impartial and independent of any Stakeholder Group or Member affiliations. (2.2.2)

## 2.2.1. Identity Ecosystem Plenary

### Composition

The NOI sought to determine what structures could be established to support the creation and adoption of policies, procedures, and standards necessary to govern the Identity Ecosystem. In response to this query, many NOI respondents stated that in order for the Plenary to successfully carry out the complex work assignments of the Steering Group, it would be necessary to establish focused committees and working groups with dedicated and qualified members.<sup>37, 38</sup> Collectively, these committees and working groups would review and recommend technical standards for adoption, establish and maintain the policies and procedures that govern the Identity Ecosystem, develop and establish accountability measures to promote broad adherence to these procedures, and facilitate the ongoing operation of the Steering Group. Support for such a structure can be found in

<sup>37</sup> Federal Register, Vol. 76, No. 114 (June 14, 2011): p. 34652.

<sup>38</sup> See, e.g., Daon at 4,6,9, EDUCAUSE/Internet2/InCommon at 3-4, Inman Technologies at 2, Kantara 4-5, Unisys at 1-3, Financial Services Sector Council for Critical Infrastructure Protection and Homeland Security at 2, Transglobal Secure Collaboration Platform at 3, and Deloitte & Touche LLP at 3, Response to NIST NOI.

several NOI responses that specified the need for working groups and committees that could focus their efforts on specific aspects of the development of standards, policies, and procedures.<sup>39</sup>

In particular, one respondent stated that the Plenary should be organized into “functional groups.”<sup>40</sup> Additional respondents suggested that there should be permanent structures in place to conduct the work outlined in the Strategy, maintain alignment with the NSTIC Guiding Principles, and to protect individual Identity Ecosystem participants.<sup>41</sup>

**Recommendation 11:** The Identity Ecosystem Plenary should include Standing Committees and Working Groups, dedicated to performing the work of the Steering Group. Standing Committees should be created to coordinate ongoing and/or permanent activities that occur within the Plenary. In addition to Standing Committees, more agile and ad hoc Working Groups should be established to conduct the work necessary for standards adoption and policy development/implementation as needed. These groups should be created as the Plenary or Management Council sees fit and should be open to all members of the Identity Ecosystem Steering Group.

**Recommendation 12:** Each Working Group and Standing Committee should establish its own charter to outline their organization, resources, processes, and missions.

**Recommendation 13:** The individual Working Group and Standing Committee charters should be reviewed and approved by the Management Council to confirm appropriate resources will be allocated, that balanced representation will be achieved, and that the NSTIC Guiding Principles will be taken into account during establishment.

**Recommendation 14:** Standing Committees should be established that are directly aligned with Steering Group responsibilities outlined in the NSTIC<sup>42</sup>, including:

- **Policy Coordination Committee.** The Policy Coordination Committee should be responsible for coordinating policies to facilitate and promote the establishment of the Identity Ecosystem and the rules for participation.
- **Standards Coordination Committee.** The Standards Coordination Committee should be responsible for coordinating, reviewing, and recommending the adoption of technical standards to facilitate interoperability within the Identity Ecosystem.
- **Accreditation Coordination Committee.** The Accreditation Coordination Committee should be responsible for coordinating accreditation requirements for Identity Ecosystem participants.

**Recommendation 15:** Two additional Standing Committees should be established to support critical responsibilities of the Steering Group:

- **Nominations Committee.** The Nominations Committee should be responsible for evaluating candidate qualifications to serve as the Chair on the Plenary and Management

---

<sup>39</sup> See, e.g., Daon at 4,6, EDUCAUSE/Internet2/InCommon at 3-4, Inman Technologies at 2, Kantara at 4-5, Unisys at 1-3, Financial Services Sector Council for Critical Infrastructure Protection and Homeland Security at 2-3, Deloitte & Touche LLP at 3, and Transglobal Secure Collaboration Platform at 3, Response to NIST NOI.

<sup>40</sup> Open Identity Exchange, Response to the NIST NOI, p. 102.

<sup>41</sup> See, e.g., Daon at 4-6, EDUCAUSE/Internet2/InCommon at 5, and Deloitte & Touche LLP at 3-4, Response to NIST NOI.

<sup>42</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, p. 31.

Council or as a Delegate (Stakeholder Group or At-Large) within the Management Council. Selection criteria should focus on visionary capability, team effectiveness, outreach, expertise, and commitment (detailed in Charter 3.2.1) to enable the selection of persons that can work for the welfare of the Identity Ecosystem as a whole, while minimizing self-interested conduct that could hinder the effectiveness and legitimacy of the Steering Group.

- **Privacy Coordination Committee.** The Privacy Coordination Committee should be responsible for seeing that other Committees' and Working Groups' work products adhere to the Privacy-enhancing and Voluntary Guiding Principle. To that end, this group should have a "gatekeeper" function; meaning no recommendations on policies, standards or other work products should be reviewed or approved by the Plenary unless first approved by the Privacy Coordination Committee. This committee should be staffed by individuals with extensive experience in the privacy field, and comprising a balance of viewpoints across a spectrum of experience, including advocacy organizations and the private sector.

Multiple respondents to the NOI supported the concept of a Privacy Coordination Committee. As one respondent noted, "In order to assure adequate privacy protections, the NSTIC governance structure...should include a special sub-group that focuses exclusively on issues with privacy. The privacy sub-group would be responsible for ensuring compliance with Fair Information Practices."<sup>43</sup> Another noted that when it comes to privacy, "It is worth mentioning the significant and powerful tension between protecting personal privacy and the desires of the marketplace to monetize personal identity. Therefore, the market alone is unlikely to force commercial entities to adhere to the guiding principles."<sup>44</sup> The gatekeeper function is critical to accomplishing these goals. SGIP also has a Privacy and Security Committee with this function that has been effective at integrating these principles into its work flow. In addition, the gatekeeper function can drive Working Groups to incorporate privacy experts into their groups or seek guidance as work products are being developed rather than waiting until the end of the process – an issue noted by one respondent.<sup>45</sup>

**Recommendation 16:** The following initial Working Groups should be established:

- **Usability and Accessibility Working Group.** The Usability and Accessibility Working Group should be responsible for evaluating technologies and identity solutions within the Identity Ecosystem to confirm that they are easy-to-use and accessible for all potential users, in accordance with the NSTIC Guiding Principles.
- **Security Working Group.** The Security Working Group should be responsible for evaluating technologies and identity solutions within the Identity Ecosystem to confirm that they meet applicable requirements for confidentiality, integrity, and availability, and are capable of timely restoration after any disruption. The work of this group should be conducted in accordance with the NSTIC Guiding Principle for the security and resilience of identity solutions.

---

<sup>43</sup> Electronic Privacy Information Center/Liberty Coalition, Response to NIST NOI, p. 9.

<sup>44</sup> EDUCAUSE/ Internet2/ InCommon, Response to NIST NOI, p. 7.

<sup>45</sup> Electronic Frontier Foundation, Response to NIST NOI, p. 4.

- **International Coordination Working Group.** The International Coordination Working Group should be responsible for reviewing– and where appropriate, coordinating alignment with – similar international identity standards and policies.

### **Membership**

Although no respondents raised the point specifically, the government recognizes a membership structure that promotes active participation is essential to the long-term sustainability of the Steering Group. At the same time, the Steering Group must remain open and accessible to a broad range of stakeholders even if these stakeholders’ capabilities for involvement may differ.

Additionally, in response to the *Initiation* section of the NOI, respondents stated that financial contributions should not determine an individual or member organization’s ability to influence the decision making process within the Steering Group.<sup>46</sup> Membership should instead be based upon the degree of participation an organization or individual is capable of providing to the Steering Group. Adopting a system that bases voting on Plenary work, and maintains an observational level of membership, allows the Steering Group to promote active participation while remaining open to those who are not capable of regular participation. This method of membership distinction is currently in use by SGIP, whose organizational structure, as previously mentioned, received significant support from NOI respondents.

**Recommendation 17:** Steering Group members within the Plenary should be designated as either Participating Members or Observing Members.

- **Participating Members.** Participating Members should be those stakeholders who actively participate in the Steering Group and the work of the Plenary, its Standing Committees, and Working Groups. Participating Members should have a vote in all Plenary proceedings. The criteria for active participation such as attendance quotas or other measurable conduct should be defined in the By-Laws established during the initiation of the Steering Group.
- **Observing Members.** Observing Members should be those stakeholders who do not meet the criteria for active participation, but want to maintain a presence in the Steering Group. Observing Members may still contribute to the work of the Plenary, its Standing Committees, and Working Groups, but they should not be permitted to vote in the Plenary.

Safeguarding against undue influence is an important consideration for providing all stakeholder groups with adequate and fair representation as well as legitimacy for the Steering Group. One NOI response noted the importance of safeguarding against one organization holding undue influence, stating, “No one community should be able to veto or hold sway over others...”<sup>47</sup>

**Recommendation 18:** Each Participating Member should receive only one vote in Plenary proceedings. Each Participating Member should select a single individual to represent them in all Plenary votes.<sup>48</sup> Adopting this concept would help support balanced representation regardless of

---

<sup>46</sup> See, e.g., Jericho Forum at 6, Online Trust Alliance at 2, Open Identity Exchange at 57, Smart Card Alliance at 1-3,6, and Verizon at 2, Response to NIST NOI.

<sup>47</sup> EDUCAUSE/Internet2/InCommon, Response to NIST NOI, p. 5.

<sup>48</sup> Plenary votes are distinct from informal voting that may be part of participants’ decision making in Committees or Working Groups.



stakeholder size or financial and material resources. Large organizations would not be able to flood the Plenary with individual voters and dominate decision making.

An organizational member, whether participating or observing, may have multiple affiliated individuals active within the Plenary.<sup>49</sup> For example, a large organization may have ten employees who participate in different Working Groups and Standing Committees depending on their expertise. However, that organization, assuming it was a Participating Member, should only be considered a single member with one Plenary vote.

By limiting each Participating Member to one voting representative, the Steering Group could better limit any one organization from exerting undue influence.

### **Leadership**

Finally, a few NOI respondents pointed out that effective leadership must be established within the Steering Group.<sup>50</sup>

**Recommendation 19:** A Plenary Chair position should be adopted to manage meetings, supervise votes/elections, and provide leadership to the Plenary.

## **2.2.2. Identity Ecosystem Management Council**

### **Size**

A significant number of the responses emphasized that the Management Council (referred to using a variety of different terms in the NOI responses) needed to be relatively small in size (9-20 members) to maintain agility.<sup>51</sup> A particular NOI response specified that the Management Council must be, “multi-sector” and “multi-faceted” and include “balanced representation” of all the Identity Ecosystem’s Stakeholders.<sup>52</sup>

**Recommendation 20:** The Management Council should consist of one representative (Management Council Delegate) from each of the 14 stakeholder groups (defined in Section 2.3), selected through an established election process.

**Recommendation 21:** These delegates should be allotted a single vote on behalf of their stakeholder group in all Management Council proceedings. This approach would maximize agility and prevent any “one community” from being able “to veto or hold sway over others”.<sup>53</sup>

**Recommendation 22:** The Management Council should maintain two at-large seats with full voting rights, to represent the interests of the Steering Group as a whole.<sup>54</sup> As with all other Delegate seats, the At-Large candidates should be approved by the Nominations Committee.

---

<sup>49</sup> Because the output of the Committees and Working Groups will have broad impact on the direction of the Identity Ecosystem, the definition of an affiliated individual may need to be addressed in the By-laws to further constrain the potential for undue influence by an organization.

<sup>50</sup> Daon, Response to NIST NOI, p. 8.

<sup>51</sup> See, e.g., Timothy Jergensen at 10, vDesk at 1-2, International Biometrics & Identification Association at 1, IBM at 3-4, Kaliya Hamlin at 21, and Electronic Privacy Information Center /Liberty Coalition at 4, Response to NIST NOI.

<sup>52</sup> vDesk, Response to NIST NOI, p. 2.

<sup>53</sup> EDUCAUSE, Internet2, InCommon, Response to NIST NOI, p. 5.

## **Officers**

Two respondents specified that the Management Council should be “composed of a set of officers & at-large members”<sup>55</sup> who should exhibit, “constitutional awareness, a commitment to fairness and justice, a commitment to transparency, innovativeness, insightfulness, pragmatism (in particular, the ability to recognize the realities of business and value propositions), multidisciplinary expertise, the ability to catalyze business models, the ability to drive toward goals and deliverables (which should be clearly defined), and an international perspective.”<sup>56</sup>

A respondent further stated that at the head of this structure should sit someone who is both a “luminary leader” and a “strong executive director” tasked with guiding the actions of the Steering Group.<sup>57</sup> Several responses noted that officers and the representatives should be selected through an open or peer election process.<sup>58</sup> One respondent also suggested in their response that the Steering Group should create an officer dedicated to coordinating Identity Ecosystem activities with the NSTIC Guiding Principles.<sup>59</sup>

**Recommendation 23:** The following three non-voting officers should be created:

- **The Chair.** The Chair should provide general leadership to the Management Council; oversee votes, and direct meetings of the Management Council. The Chair should be selected through a general election of Participating Members in the Plenary. Voting through the Plenary rather than the Management Council would ensure that one Stakeholder group will not lose the representation of its voting Delegate for the Chair’s term.
- **The Vice-Chair.** The Vice-Chair should facilitate the Steering Group’s work towards successful implementation of the NSTIC and alignment with the NSTIC Guiding Principles. The position of Vice-Chair should be filled by the Director of the National Program Office. As outlined in NSTIC, the National Program Office’s responsibilities are in part: to promote private-sector involvement and engagement, build consensus on policy frameworks necessary to achieve the vision, actively participate within and across relevant public and private sector fora, and assess progress against the goals, objectives, and milestones of the Strategy.<sup>60</sup> Note that the Vice-Chair would have a separate set of responsibilities from U.S. government agency stakeholders – focused not on advocating for U.S. government interests, but on behalf of the NSTIC itself.

A key tenet expressed in the Strategy is protection and representation for the rights of individuals within the Identity Ecosystem. A number of NOI respondents supported this position and cited the

---

<sup>54</sup> Daon, Response to NIST NOI, pp. 3-4.

<sup>55</sup> Daon, Response to NIST NOI, p. 8.

<sup>56</sup> Microsoft, Response to NIST NOI, p. 7.

<sup>57</sup> Daon, Response to NIST NOI, p. 8.

<sup>58</sup> See, e.g., Smart Card Alliance at 3.5, and Kaliya Hamlin at 21, Response to NIST NOI.

<sup>59</sup> IBM, Response to NIST NOI, p. 3.

<sup>60</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, p. 39.

responsibility of the Steering Group to create a structure that provides adequate protection for the individual as a means of garnering public trust.<sup>61</sup> Several respondents stated the need for an officer whose sole responsibility would be safeguarding the representation and protection of individual rights.<sup>62</sup> As an additional measure for supporting alignment with the NSTIC Guiding Principles and adequately representing the needs of the entire stakeholder population, an unbiased representative should be present on the Management Council.

- **The Ombudsman.** The Ombudsman should be responsible for upholding the NSTIC Guiding Principles and Steering Group charter, representing and advocating for consumers or other individuals and underrepresented groups, safeguarding against individual stakeholder groups exerting excessive influence, monitoring and reporting on Management Council activities, managing grievances from the Plenary, and facilitating public comment and citizen outreach. This position should not be selected from one of the existing stakeholder groups or members, but should instead be provided by the Secretariat; allowing the Ombudsman to maximize independence and impartiality in executing his or her duties. The criteria for selection should be established by the Management Council.

## **2.3. Stakeholder Representation**

### **Stakeholder Groups**

The Strategy calls for the Steering Group to bring together representatives of all of the interested stakeholders of the Identity Ecosystem. Given the large number of stakeholders in the Identity Ecosystem, it is especially important to find ways to adequately balance the diverse interests of the various stakeholders. The NOI included a number of questions in the NOI that were focused exclusively on how the Steering Group could achieve such balanced representation, including how to sufficiently represent individuals, preserve personal privacy, and be accessible to stakeholders that may have limited availability and/or resources to participate.<sup>63</sup>

In addressing these questions, many NOI respondents agreed that the interests of all stakeholders should be represented in the Steering Group.<sup>64</sup> A specific NOI response noted the disparate requirements of Identity Ecosystem stakeholders, stating, “Stakeholder representation needs to be diverse. It must represent all the different service providers within the Identity Ecosystem (e.g., identity providers, attribute providers, relying parties, accreditation authorities); represent different industries, which often have different business drivers and regulations (e.g., healthcare, financial sector, Federal Government); and represent different functional and technical competencies (e.g., legal, expertise in technologies, privacy, consumer advocacy, economic, etc.)”<sup>65</sup> Several NOI

---

<sup>61</sup> See, e.g., Civics.com at 3, EDUCAUSE/Internet2/InCommon at 8-9, Timothy Jurgensen at 4-5, Deloitte & Touche LLP at 3-8, and Smart Card Alliance at 3, Response to NIST NOI.

<sup>62</sup> See, e.g., Microsoft at 3, U.S. Public Policy Council of the Association for Computing Machinery at 2, Response to NIST NOI.

<sup>63</sup> Federal Register, Vol. 76, No. 114 (June 14, 2011): pp. 34652-34653.

<sup>64</sup> See, e.g., Civics at 3, Daon at 2,4, EDUCAUSE, Internet2, InCommon at 8-9 The Jericho Forum at 9-10, and The Transglobal Secure Collaboration Program at 7, Response to NIST NOI.

<sup>65</sup> Deloitte & Touche LLP, Response to NIST NOI, p 4.

respondents also stated that specific industry segments, portions of the population, and standards development organizations should be recognized as individual stakeholder groups.<sup>66</sup>

NSTIC focuses primarily on the roles of participants in the Identity Ecosystem as well as the Guiding Principles necessary to sustain it. A Steering Group that reflects this focus will be able to encompass the interests of all stakeholders in a manner that best supports the welfare of the Identity Ecosystem as a whole.

Accordingly, a Management Council comprised of representatives that generally reflect the roles of Identity Ecosystem participants and the Guiding Principles offers the most optimal structure for a Council. Sector or industry specific concerns can be most effectively addressed within the Working Groups of the Plenary, discussed in Section 2.2. Additionally, sector associated stakeholder groups often fluctuate as markets, technologies, and trends modify the environment.

By organizing the stakeholder groups according to responsibilities and roles, and not by sector, the Steering Group can allow the number of groups to remain limited and manageable.

**Recommendation 24:** Fourteen stakeholder groups should be designated within the Steering Group for the purpose of electing Delegates to the Management Council; designation of these groups would have no impact on operations in the Plenary, the Working Groups, or the Standing Committees.

**Recommendation 25:** Each Stakeholder should be required to “self-identify” into the stakeholder group which it considers best represents its primary role or interest in the Identity Ecosystem. Self-identification into one stakeholder category at a time would prevent organizations that may play multiple roles in the Identity Ecosystem from exerting undue influence by gaining more than one vote on the Management Council. Importantly, individuals that do not wish to self-identify into one of the other 13 stakeholder groups may choose to participate as an Unaffiliated Individual. The 14 recommended stakeholder groups are:

- **Privacy & Civil Liberties.** This group would focus on the protection of individuals’ privacy and civil liberties.
- **Usability & Human Factors.** This group would focus on technologies and solutions that are usable and incorporate the human, cognitive, and social properties unique to the characteristics of humans.
- **Consumer Advocates.** This group would focus on addressing the interests and accessibility of consumers and other individual end-user populations.
- **U.S. Federal Government.** This group would focus on the interests of the departments and agencies that comprise the U.S. Federal Government. Under its various forms and component programs, the government may act as an identity provider, attribute provider, and relying party. This group’s Management Council Delegate would be responsible for advocating for the Federal Government as a Stakeholder; unlike the Vice-Chair who would advocate on behalf of the NSTIC itself.
- **U.S. State, Local, Tribal, and Territorial Government.** This group would focus on the interests of the various state, local, tribal, and territorial governments that exist within the U.S.

---

<sup>66</sup> See, e.g., Aetna and Medicity at 1, Smart Card Alliance at 5, Kaliya Hamlin at 40, and Financial Services Sector Council for Critical Infrastructure Protection and Homeland Security at 2,3, Response to NIST NOI.

- **Research, Development & Innovation.** This group would focus on research and technology development in support of the Identity Ecosystem.
- **Identity & Attribute Providers.** This group would focus on the processes and technologies associated with establishing, managing, and securing digital identities and attributes.
- **Interoperability.** This group focuses on supporting interoperability within the Identity Ecosystem, inclusive of Trust Framework Providers and standards development organizations.
- **Information Technology (IT) Infrastructure.** This group would focus on IT infrastructure relevant to the functioning of the Identity Ecosystem, inclusive of different types of communications and network traffic, as well as virtual and distributed functions that produce and provide hardware, software, and IT systems and services.
- **Regulated Industries.** This group would focus on industries covered by sector-specific regulations that may be affected by the development of the Identity Ecosystem Framework.
- **Small Business & Entrepreneurs.** This group would focus on the impact of the development of the Identity Ecosystem Framework on small businesses and individual business owners/operators.
- **Security.** This group would focus on IT security services that support the confidentiality, integrity, and availability of identity solutions
- **Relying Parties.** This group would focus on transaction decisions based upon receipt, validation, and acceptance of an entity's authenticated credential(s) and identity attributes.
- **Unaffiliated Individuals.** This group would consist of any individual who does not self-identify into one of the other stakeholder groups.

### Consensus

In addition to the composition of stakeholder categories, organizational process can be used to accommodate many different perspectives and sets of stakeholders. For instance, multiple NOI respondents suggested that the Steering Group adopt a consensus driven process.<sup>67</sup> In particular, one respondent specified the need for a consensus-driven process backed by a small group of leaders elected by the Plenary.<sup>68</sup>

**Recommendation 26:** A consensus-driven process should be implemented that uses due diligence including, but not limited to, evidence gathering through research, demonstrations, proofs of concept, evaluations, and surveys to explore differing options to general agreement and acceptance among stakeholders. This process should be used at all levels of the Steering Group from working groups to the Management Council.

**Recommendation 27:** Voting, through a defined process, should be used when consensus is not attainable.

---

<sup>67</sup> See, e.g., vDesk at 8-9, Verizon at appendix A, United States Chamber of Commerce at 2-4, Electronic Frontier Foundation at 4, Jericho Forum at 6, Open Identity Exchange at 84-86, The Open Group at 2, Visa at 1, Deloitte & Touche LLP at 5-6, and IBM at 3, Response to NIST NOI.

<sup>68</sup> United States Chamber of Commerce response to the NIST NOI, pp. 2-4.

## **Operating Principles**

Along with a consensus driven process, NOI respondents strongly supported the principle that the Steering Group conduct itself in a manner that is open and transparent. Operating in this manner allows all stakeholders, especially those that may have fewer resources, to have an opportunity to participate. Two respondents in particular emphasized the point. The first stated, “All records...should be open to the public through a website; recommendations or suggestions from the public should be welcomed at public meetings and through the website and tracked for internal accountability.”<sup>69</sup> The other respondent noted the Steering Group would, “have questionable legitimacy” if it did not operate in a way that was “open and genuinely representative of users.”<sup>70</sup> This respondent went on to suggest that “deliberations” should “take place on-line” and that there should be staff, “specifically devoted to helping make steering group activities more transparent and accessible.”<sup>71</sup>

**Recommendation 28:** The Steering Group should conduct all operations and administrative actions in an open and transparent manner including, but not limited to, taking the following steps:

- All meetings should be open for public attendance, virtually or physically;
- Identity Ecosystem documents should be publicly available and posted to an easily accessible website; and
- Technologies should be leveraged to create user-friendly and broad avenues for participation in all proceedings and administrative functions.
- The Secretariat should be specifically charged with providing staff and services to maintain the Steering Group’s objectives of openness and transparency.

By establishing a set of operating principles, the Steering Group can create an effective, participatory, and accountable governance structure.

**Recommendation 29:** The Steering Group should adhere to the following Operating Principles, as defined in the Recommended Charter:

- Openness and Transparency
- Balance
- Consensus
- Harmonization

While every member of the Steering Group should play an important role in maintaining these Operating Principles, the Secretariat (2.1), the Management Council Vice-Chair (2.2.2), and the Ombudsman (2.2.2) should have primary responsibility for maintaining alignment with the principles outlined above.

## **Participation**

As part of establishing an open and transparent environment, the Identity Ecosystem Steering Group should create the opportunity for multiple pathways to participation. The NOI

---

<sup>69</sup> Daon, Response to NIST NOI, p. 10.

<sup>70</sup> Electronic Frontier Foundation, Response to NIST NOI, p. 3.

<sup>71</sup> Electronic Frontier Foundation, Response to NIST NOI, pp. 3-4.

acknowledged that not all stakeholders will have the time and resources available to directly participate in the Steering Group's operations (e.g., committees and working groups within the Plenary). While not all of the NOI responses addressed this issue directly, one particular NOI response noted several potential options that would allow Identity Ecosystem participants the opportunity to interact with and influence the decision-making process.

Below are a few examples of avenues for participation as noted in one NOI response:<sup>72</sup>

- **Directly participate in the Identity Ecosystem Steering Group.** Identity Ecosystem participants may join the Plenary and participate or observe its operations, thereby becoming directly involved in the ongoing operations and management of the Identity Ecosystem Framework.
- **Participate and comment in a Trust Framework.** The Identity Ecosystem contains many Trust Frameworks. Participants within individual Trust Frameworks may provide feedback on the Identity Ecosystem and Identity Ecosystem Framework through their Trust Framework Provider.
- **Participate through publicly available knowledge centers or online tools.** The activities and operations of the Steering Group should be transparent and open to the public. Therefore interested parties should be free to provide comments and feedback through a variety of forums, available to the public, without directly participating in the Steering Group.
- **Participate through Sector Associations.** The Identity Ecosystem Steering Group will contain many different sector associations. Members of these associations may be able to provide feedback on the Identity Ecosystem Framework through their sector association.

**Recommendation 30:** The Steering Group should provide multiple pathways for stakeholder participation.

### **Privacy and Stakeholder Protection**

Another NOI response that focused on providing privacy and protections for groups and individuals that may lack the resources or availability to be heavily involved in the operation of the Steering Group noted that, "The mere fact that consumer and privacy groups are represented does not mean that they will be able to adequately represent their constituencies. Without significant representation reinforcing safeguards, consumer and privacy interests are likely to be under-represented."<sup>73</sup>

We acknowledge that individual and stakeholder confidence in the protection and privacy of the Identity Ecosystem is essential to its eventual adoption and success. For this reason, this report describes multiple safeguards that are designed to work in concert to provide protections for individual privacy and the underrepresented, and guard against undue influence by any one stakeholder group. The safeguards called for throughout this paper are reflected in multiple recommendations, including:

---

<sup>72</sup> Open Identity Exchange, Response to the NIST NOI, pp. 29-32.

<sup>73</sup> Electronic Frontier Foundation, Response to NIST NOI, p. 2.

- **Privacy Coordination Committee.** The Privacy Coordination Committee, comprising a balanced and experienced body of individuals, should be responsible for reviewing all policies, standards, and technical solutions for their adherence to the NSTIC’s Guiding Principle on Privacy. No recommendations should be reviewed or approved by the Plenary unless first approved by the Privacy Coordination Committee. (Section 2.2.1)
- **The Secretariat.** As part of its administrative duties, the Secretariat should align Steering Group operations with the Charter’s Operating Principles (Section 2.1)
- **The Ombudsman.** This officer should have multiple responsibilities, however, his or her primary role should be to act as an advocate for underrepresented stakeholders, and support balanced representation in the Steering Group. Any individual or organization with grievances could present them to the Ombudsman for discussion and adjudication by the Steering Group. This position should be independent of any stakeholder affiliations. (Section 2.2.2)
- **The Vice-Chair.** This position should be filled by the Director of the NSTIC National Program Office and among other things, should be responsible for advocating for the NSTIC itself and the Guiding Principles contained therein. (Section 2.2.2)
- **Operating Principles.** All operations within the Steering Group should be conducted in accordance with the principles of openness, transparency, balance, consensus, and harmonization. In addition to allowing for effective operations, these principles should assure that the Steering Group remains accountable to the participants, members, and stakeholders of the Identity Ecosystem. (Section 2.3)
- **One Participating Member, One Vote.** To provide balance and prevent any single stakeholder, member, or sector from exercising undue influence over the Steering Group each Participating Member should have just one vote within the Plenary. Likewise, each stakeholder group will have just one Management Council Delegate, and therefore a single vote on the Management Council as well. (Section 2.2.1 and 2.2.2)
- **Pathways to Participation.** The Identity Ecosystem Steering Group should maintain multiple pathways to allow all stakeholders the broadest opportunity to take part – directly or indirectly – in the Steering Group. (Section 2.3)

## 2.4. International Coordination

### Participation

Given the global nature of online commerce, the Identity Ecosystem cannot be isolated from internationally available online services and their identity solutions. In our NOI, we sought input from the public on how the structure of the Steering Group could address international perspectives.<sup>74</sup> Several NOI respondents noted that international participants should be welcomed and encouraged to participate as they will likely bring fresh ideas and different perspectives.<sup>75</sup>

**Recommendation 31:** The Identity Ecosystem Steering Group should take steps to coordinate with the international community and encourage participation from international entities to the greatest

---

<sup>74</sup> Federal Register, Vol. 76, No. 114 (June 14, 2011): p. 34653.

<sup>75</sup> See, e.g., Certipath at 5-6, Inman Technologies at 7, OASIS at 7, and The Transglobal Secure Collaboration Program at 8-9, Response to the NIST NOI.



extent possible. At the same time, in keeping with recommendation 25 that stakeholder categories focus on Identity Ecosystem participant roles and the NSTIC Guiding Principles, a separate stakeholder category for international members should not be created. Rather, international members should self-identify into the most relevant of the 14 stakeholder categories (see 2.3) and participate in the recommended International Coordination Working Group (see 2.2.1).

### **Standards and Interoperability**

The NOI also sought public input on how the Steering Group could coordinate with similar efforts abroad and maximize the Identity Ecosystem's interoperability internationally.<sup>76</sup> In response to this request, a number of respondents felt that the Steering Group should coordinate with internationally-focused standards development organizations in an effort to achieve international acceptance of the Identity Ecosystem.<sup>77</sup> Of note, no NOI respondents advocated for the Steering Group to exclude international participants or eschew efforts at international alignment.

**Recommendation 32:** The Steering Group should coordinate with representatives from international identity initiatives, standards development organizations, trade organizations, and the international departments of member entities in order to leverage lessons learned and broadly recognized technical standards.

**Recommendation 33:** The Steering Group should strive to identify and use internationally recognized policies and standards that meet applicable assessment criteria and conform to the NSTIC Guiding Principles.

## **2.5. Recommended Steering Group Charter**

To accelerate the launch of the Steering Group and to encapsulate the recommendations contained in Section 2, we have produced a Recommended Identity Ecosystem Steering Group Charter that outlines the basic framework within which the Steering Group may operate (see Appendix B). This Charter is intended to be a standalone document that will be maintained by the Steering Group following its initiation. It outlines the Steering Group's purpose, composition, membership, member selection criteria, and scope of activities.

---

<sup>76</sup> Federal Register, Vol. 76, No. 114 (June 14, 2011): p. 34653.

<sup>77</sup> See, e.g., Internet Society at 3-4, OASIS at 7, The Transglobal Secure Collaboration Program at 8-9, vDesk at 10, Smart Card Alliance at 1, 8, and Daon at 9, Response to NIST NOI.

### **3. The Road Ahead**

The NSTIC National Program Office is committed to the Strategy and to fostering the development of the Identity Ecosystem. Subject to public comment and finalization of the approach outlined in this paper, we intend to fund, through a competitive grant, a Secretariat to convene the initial Steering Group, provide it with administrative services, material support, and logistical assistance, and maintain openness and transparency in all Steering Group activities. The Federal Funding Opportunity for this grant may be published before the final report.

Additionally, we are including a recommended Charter with this paper to help streamline the list of activities needed to formally establish the Steering Group. As the private sector establishes Steering Group operations, the NSTIC NPO will work to continue to align Federal Government activities with the NSTIC and the Guiding Principles identified in the Strategy.

## Appendix A – Steering Group Recommendations Summary

The following table contains a summary of all of the government’s recommendations for establishment of the Identity Ecosystem Steering Group. See Section 2 for additional details related to each of these recommendations.

<b>Summary of Steering Group Recommendations</b>			
<b>Steering Group Initiation Recommendations</b>			
<b>Section</b>	<b>Number</b>	<b>Recommendation Title</b>	<b>Recommendation description</b>
2.1	01	Steering Group Organization	Given the unique and complex nature of the Identity Ecosystem and the role the NSTIC envisions the government playing in its formation, the Steering Group should be established as a new organization to be led by the private sector.
	02	Establishment of the Secretariat	The Secretariat service will be funded by NIST through a competitive grant.
	03	Role of the Secretariat	The Secretariat will be charged with convening the initial meeting of the Steering Group, including providing administrative services and material support to the Steering Group (including the Working Groups and Standing Committees) and maintaining openness and transparency in all Steering Group functions, all with an eye toward aligning the Steering Group’s operations with the NSTIC Guiding Principles.
	04	Self-Sustaining Funding Models	The Steering Group should conduct an analysis of potential self-sustaining funding models which should be implemented following a period of initial support from the Federal Government.
	05	Fees	To support fair representation among stakeholders with varied resources, there should be no correlation between fees charged to Steering Group participants and the ability to vote or impact decision-making within the Steering Group.
<b>Steering Group Structure Recommendations</b>			
<b>Section</b>	<b>Number</b>	<b>Recommendation Title</b>	<b>Recommendation description</b>
2.2	06	Two Tiered Governance Model	The Steering Group should be established as a two-tiered structure.
	07	The Plenary	The Identity Ecosystem Plenary should be established to review and recommend technical standards for adoption, establish and maintain the policies and procedures that govern the Identity Ecosystem, develop and establish accountability measures to promote broad adherence to these procedures, and facilitate the ongoing operation of the Steering Group.
	08	Open Plenary Structure	The Plenary should be open to all stakeholders and individuals who wish to participate in the Identity Ecosystem Steering Group.

Recommendations for Establishing an Identity  
Ecosystem Governance Structure

	09	The Management Council	The Identity Ecosystem Management Council should be created to provide guidance to the Plenary on the broad perspectives envisioned by the Strategy; produce, prioritize and monitor progress of Steering Group work plans; provide necessary resources, and ensure that Steering Group work activities adhere to the NSTIC Guiding Principles and Goals; and ratify policy and standards recommendations approved by the Plenary.
	10	Dispersed Decision Making Authority	Decision-making authority should be divided between the two groups, with the Plenary responsible for reviewing and approving standards and policies within its working groups and committees and the Management Council ratifying those standards and policies based on the recommendation of the Plenary.
2.2.1	11	The Composition of the Plenary	The Identity Ecosystem Plenary should include Standing Committees and Working Groups, dedicated to performing the work of the Steering Group. Standing Committees should be created to coordinate ongoing and/or permanent activities that occur within the Plenary. In addition to Standing Committees, more agile and ad hoc Working Groups should be established to conduct the work necessary for standards adoption and policy development/implementation as needed. These groups should be created as the Plenary or Management Council sees fit and should be open to all members of the Identity Ecosystem Steering Group.
	12	Working Group and Standing Committee Charters	Each Working Group and Standing Committee should establish its own charter to outline their organization, resources, processes, and missions.
	13	Charter Approval	The individual Working Group and Standing Committee charters should be reviewed and approved by the Management Council to confirm appropriate resources will be allocated, that balanced representation will be achieved, and that the NSTIC Guiding Principles will be taken into account during establishment.
	14	NSTIC Aligned Standing Committees	Standing Committees should be established that are directly aligned with Steering Group responsibilities outlined in the NSTIC including: The Policy Coordination Committee, The Standards Coordination Committee, and the Accreditation Coordination Committee.
	15	Additional Standing Committees	Two additional Standing Committees should be established to support critical responsibilities of the Steering Group: The Nomination Committee and the Privacy Coordination Committee (this committee will have a gatekeeper function)
	16	Initial Working Groups	The following initial Working Groups should be established: The Usability and Accessibility Working Group, The Security Working Group, and The International Coordination Working Group

Recommendations for Establishing an Identity  
Ecosystem Governance Structure

	17	Membership Designations	Steering Group members within the Plenary should be designated as either Participating Members (with voting privileges) or Observing Members (without voting privileges).
	18	One Participating, Member One Vote	Each Participating Member should receive only one vote in Plenary proceedings. Each Participating Member should select a single individual to represent them in all Plenary votes.
	19	The Plenary Chair	A Plenary Chair position should be adopted to manage meetings, supervise votes/elections, and provide leadership to the Plenary.
2.2.2	20	Management Council Composition	The Management Council should consist of one representative (Management Council Delegate) from each of the 14 stakeholder groups (defined in Section 2.3), selected through an established election process.
	21	One Delegate, One Vote	These delegates should be allotted a single vote on behalf of their stakeholder group in all Management Council proceedings.
	22	At-Large Delegates	The Management Council should maintain two at-large seats with full voting rights, to represent the interests of the Steering Group as a whole. As with all other Delegate seats, the At-Large candidates should be approved by the Nominations Committee.
	23	Officers	The following three non-voting officers should be created: the Chair; the Vice-Chair (should be filled by the director of NSTIC NPO), and the Ombudsman.
<b>Stakeholder Representation Recommendations</b>			
<b>Section</b>	<b>Number</b>	<b>Recommendation Title</b>	<b>Recommendation description</b>
2.3	24	Stakeholder Group Representation	Fourteen stakeholder groups should be designated within the Steering Group for the purpose of electing Delegates to the Management Council; designation of these groups would have no impact on operations in the Plenary, the Working Groups, or the Standing Committees.
	25	Stakeholder Groups	Each Stakeholder should be required to “self-identify” into the stakeholder group which it considers best represents its primary role or interest in the Identity Ecosystem. Individuals that do not wish to self-identify into one of the other 13 stakeholder groups may choose to participate as an Unaffiliated Individual. The 14 recommended stakeholder groups are: Privacy and Civil Liberties, Usability & Human Factors, Consumer Advocates, U.S. Federal Government, U.S. State, Local, Tribal, and Territorial Government, Research, Development, & Innovation, Identity & Attribute Providers, Interoperability, Information Technology Infrastructure, Regulated Industries, Small Business & Entrepreneurs, Security, Relying Parties, and Unaffiliated Individuals.

Recommendations for Establishing an Identity  
Ecosystem Governance Structure

	26	Consensus Based Decision Making	A consensus-driven process should be implemented that uses due diligence including, but not limited to, evidence gathering through research, demonstrations, proofs of concept, evaluations, and surveys to explore differing options to general agreement and acceptance among stakeholders. This process should be used at all levels of the Steering Group from working groups to the Management Council.
	27	Voting	Voting, through a defined process, should be used when consensus is not attainable.
	28	Transparency and Openness	The Steering Group should conduct all operations and administrative actions in an open and transparent manner.
	29	Operating Principles	The Steering Group should adhere to the following Operating Principles, as defined in the Recommended Charter: Openness and Transparency, Balance, Consensus, and Harmonization.
	30	Pathways to Participation	The Steering Group should provide multiple pathways for stakeholder participation.
<b>International Coordination Recommendations</b>			
<b>Section</b>	<b>Number</b>	<b>Recommendation Title</b>	<b>Recommendation description</b>
2.4	31	International Entity Participation	The Identity Ecosystem Steering Group should take steps to coordinate with the international community and encourage participation from international entities to the greatest extent possible. At the same time, in keeping with recommendation 26 that stakeholder categories focus on Identity Ecosystem participant roles and the NSTIC Guiding Principles, a separate stakeholder category for international members should not be created. Rather, international members should self-identify into the most relevant of the 14 stakeholder categories (see 2.3) and participate in the recommended International Coordination Working Group (see 2.2.1).
	32	Coordination with International Efforts	The Steering Group should coordinate with representatives from international identity initiatives, standards development organizations, trade organizations, and the international departments of member entities in order to leverage lessons learned and broadly recognized technical standards.
	33	Use of Internationally-Recognized Policies and Standards	The Steering Group should strive to identify and use internationally recognized policies and standards that meet applicable assessment criteria and conform to the NSTIC Guiding Principles.

## **Appendix B – Recommended Identity Ecosystem Steering Group Charter**

# **RECOMMENDED CHARTER FOR THE IDENTITY ECOSYSTEM STEERING GROUP**

---

## 1. Identity Ecosystem Steering Group Charter

The National Strategy for Trusted Identities in Cyberspace (NSTIC or Strategy), signed by President Obama in April 2011, acknowledges and addresses a major weakness in cyberspace – a lack of confidence and assurance that people, organizations, and businesses are who they say they are online.<sup>78</sup> Additionally, in the current online environment, individuals are asked to maintain dozens of different usernames and passwords, one for each website with which they interact. The complexity of this approach is a burden to individuals, and it encourages behavior – such as the reuse of passwords – that makes online fraud and identity theft easier. At the same time, online businesses are faced with ever-increasing costs for managing customer accounts, the consequences of online fraud, and the loss of business that results from individuals’ unwillingness to create yet another account. Moreover, both businesses and governments are unable to offer many services online, because they cannot effectively identify the individuals with whom they interact. Spoofed websites, stolen passwords, and compromised accounts are all symptoms of inadequate authentication mechanisms.<sup>79</sup>

The Identity Ecosystem envisioned in the NSTIC is an online environment that will enable people to validate their identities securely, but with minimized disclosure of personal information when they are conducting transactions. The vibrant marketplace created by the Identity Ecosystem will provide people with choices among multiple accredited identity providers, both private and public, and choices among multiple credentials. For example, imagine that a student could get a digital credential from her cell phone provider and another one from her university and use either of them to log-in to her bank’s website, her e-mail, three social networking sites, four online commerce sites, and so on, all without having to remember dozens of passwords. The added convenience, security, and privacy provided within the Identity Ecosystem will allow additional services to be put online to drive greater economic growth. Notwithstanding the objective to improve identification and authentication in cyberspace for certain types of transactions, not all Internet activities have such needs. Thus, the capacity for anonymity and pseudonymity will be maintained in the envisioned Identity Ecosystem.

A core tenet of the NSTIC is that its implementation must be led by the private sector. The NSTIC calls for the Federal Government to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the processes by which online transactions are conducted. The Strategy itself was developed with substantial input from both the private sector and the American public. The National Institute of Standards and Technology (NIST), which has been designated to establish a National Program Office to lead the implementation of the NSTIC, recognizes that a strong and vibrant public-private partnership is necessary to execute the Strategy’s vision in a way that supports the wide range of interactions that occur over the Internet. As such, NIST is leading the effort to fulfill the NSTIC’s call for government to work in close partnership with the private sector and other relevant stakeholder groups to, “[Establish a steering group to] administer the process for policy and standards development for the Identity Ecosystem Framework in accordance with the Guiding Principles in

---

<sup>78</sup> The full Strategy can be found at: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/NSTICstrategy\\_041511.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf)

<sup>79</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, 1.



[the] Strategy. The steering group will also ensure that accreditation authorities validate participants' adherence to the requirements of the Identity Ecosystem Framework."<sup>80</sup>

## **1.1. Mission**

The Mission of the Steering Group shall be to govern and administer the Identity Ecosystem Framework in a manner that stimulates the development and sustainability of the Identity Ecosystem. The Steering Group will always operate in accordance with the NSTIC's Guiding Principles.

### **1.1.1. Objectives**

The activities and work products of the Steering Group shall be conducted in support of the following objectives:

- Ensure that the Identity Ecosystem and Identity Ecosystem Framework conform to the four NSTIC Guiding Principles (as detailed in section 1.3).
- Administer the process for policy and standards development and adoption for the Identity Ecosystem Framework and, where necessary establish policies standards for the Identity Ecosystem Framework.
- Adopt and, where necessary, establish standards for the Identity Ecosystem Framework.
- Certify that accreditation authorities validate adherence to the requirements of the Identity Ecosystem Framework.

### **1.1.2. Purpose**

The purpose of the Steering Group shall be to develop and administer the process for policy and technical standards development for the Identity Ecosystem Framework. The Steering Group shall bring together all of the interested stakeholders, both in private and public sectors, to confirm that the Identity Ecosystem Framework provides a minimum baseline of privacy, security, interoperability, and ease-of-use through standards and policies, without creating unnecessary barriers to entry. The Steering Group shall facilitate the fulfillment of the NSTIC goals to develop a comprehensive Identity Ecosystem Framework; build and implement the Identity Ecosystem; enhance confidence and willingness to participate in the Identity Ecosystem; and, support the long-term success and sustainability of the Identity Ecosystem.<sup>81</sup>

The Steering Group shall not be a standards development body, but rather an organization that promotes the development of standards and develops policies that serve to accelerate the development and adoption of the Identity Ecosystem.

## **1.2. Scope of Activities**

The activities of the Steering Group shall be limited to achievement of the objectives listed in this charter. Additional activities that are not considered essential to completion of these objectives may

---

<sup>80</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, p. 25.

<sup>81</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, p. 31.

be conducted when determined appropriate through Steering Group consensus. The scope of the Steering Group's activities is summarized in the sections that follow.

### **1.2.1. Adopt and Establish Standards**

The Steering Group shall establish forums and procedures to review applicable standards and adopt those that support achievement of the NSTIC vision, conform to the Guiding Principles, and meet other established requirements. Additionally, the Steering Group will recommend standards be established when gaps are identified. The Steering Group shall advocate for standards to be established and adopted in a timely manner and be sufficient to keep pace with emerging technology and market trends.

### **1.2.2. Develop and Maintain Policies**

The Steering Group shall establish the mechanisms necessary to develop, implement, and maintain policies that are appropriate for use in the Identity Ecosystem and conform to the NSTIC Guiding Principles. The Steering Group shall support the timely development and implementation of policies.

### **1.2.3. Develop and Maintain Processes for the Accreditation of Identity Ecosystem Entities**

The Steering Group shall develop, foster, and implement a clear process for accrediting entities within the Identity Ecosystem as well as develop clear testing and certification criteria by which adherence to the recommended standards and policies may be measured.

The Steering Group shall ensure that this accreditation process is applied fairly to all Identity Ecosystem participants.

### **1.2.4. Develop and Maintain Identity Ecosystem Operating Procedures**

The Steering Group shall develop, administer, and maintain Identity Ecosystem Operating Procedures to facilitate interoperability between and among the Identity Ecosystem participants. Operating Procedures refers to the set of policies and standards created by the Steering Group as accepted baseline requirements for participating in the Identity Ecosystem Framework.

## **1.3. Adherence to the NSTIC Guiding Principles**

The Identity Ecosystem Steering Group, its components, and its members shall at all times operate in accordance with four Guiding Principles set forth in the NSTIC. They are:

**Identity solutions will be privacy-enhancing and voluntary.** The Identity Ecosystem will be grounded in a holistic, integrated implementation of the Fair Information Practice Principles to promote the creation and adoption of policies and standards that are privacy-enhancing, including the preservation of the capacity to engage in anonymous and pseudonymous activities online. Ideally, identity solutions within the Identity Ecosystem should preserve the positive privacy benefits associated with offline identity-related transactions while mitigating some of the negative privacy aspects. Finally, participation in the Identity Ecosystem will be voluntary: the government will neither mandate that individuals obtain an Identity Ecosystem credential nor that companies require Identity Ecosystem credentials from consumers as the only means to interact with them. Individuals shall be free to use an Identity Ecosystem credential of their choice, provided the credential meets

the minimum risk requirements of the relying party, or to use any non-Identity Ecosystem mechanism provided by the relying party. Individuals' participation in the Identity Ecosystem will be a day-to-day—or even a transaction-to-transaction—choice.

**Identity solutions will be secure and resilient.** Identity solutions within the Identity Ecosystem will provide secure and reliable methods of electronic authentication by being grounded in technology and security standards that are open and collaboratively developed with auditable security processes. Credentials within the Identity Ecosystem are: issued based on sound criteria for verifying the identity of individuals and devices; resistant to theft, tampering, counterfeiting, and exploitation; and issued only by providers who fulfill the necessary requirements. Identity solutions must detect when trust has been broken, be capable of timely restoration after any disruption, be able to quickly revoke and recover compromised digital identities, and be capable of adapting to the dynamic nature of technology

**Identity solutions will be interoperable.** Interoperability encourages and enables service providers to accept a wide variety of credentials and enables users to take advantage of different credentials to assert their identity online. Two types of interoperability are recognized in the Identity Ecosystem: there will be standardized, reliable credentials and identity media in widespread use in both the public and private sectors; and if an individual, device, or system presents a valid and appropriate credential, any qualified relying party is capable of accepting and verifying the credential as proof of identity and attributes.

**Identity solutions will be cost-effective and easy to use.** The Identity Ecosystem will promote identity solutions that enable individuals to use a smaller number of identity credentials across a wide array of service providers. These identity solutions must be cost-effective for users, identity and attribute providers, and relying parties. Furthermore, identity solutions should be simple to understand, intuitive, easy-to-use, and enabled by technology that requires minimal user training.<sup>82</sup>

## **1.4. Operating Principles**

The Steering Group shall adhere to the following four operating principles.

### **1.4.1. Openness and Transparency**

The work of the Steering Group, including all working groups and committees, shall facilitate broad participation and be publically accessible. The Identity Ecosystem Steering Group shall take the following steps to provide openness and transparency in all its proceedings:

- All documents, drafts, and minutes of meetings shall be posted on a publicly available Internet site.
- All meetings of all governing bodies shall be open to public attendance and leverage virtual attendance options to maximize broad and public participation.
- Technologies should be leveraged to create user-friendly and broad avenues for participation in all proceedings and administrative functions.

---

<sup>82</sup> National Strategy for Trusted Identities in Cyberspace, The White House, April 2011, 25, 11-14.

### **1.4.2. Balance**

The Steering Group shall strive to achieve balanced representation among all stakeholder groups regardless of their size, financial status, or sector alignment/affiliation.

### **1.4.3. Consensus**

Consensus—general agreement among members—shall be a core value of the Steering Group. All processes instituted by the Steering Group shall require participants to consider all views, proposals and objections, and endeavor to reconcile them. Although positions of leadership, such as committee chairs, are likely to serve as the primary drivers of consensus, all Steering Group participants must be (1) cooperative in the consensus process; (2) constructive; and (3) respectful when providing feedback or dissenting opinions. In the event that consensus cannot be reached, voting, by an established method, shall be used to make Steering Group decisions.

### **1.4.4. Harmonization**

The Steering Group shall encourage harmonization of standards and policies and shall always strive to recognize the impacts of policy and standards on all stakeholders in the Identity Ecosystem.

## **1.5. Membership**

Membership in the Steering Group shall be open to organizations and unaffiliated individuals (Members) that have an interest in the development of the Identity Ecosystem. A Member organization may have more than one individual within its organization participate in Steering Group activities; however, it shall designate only one individual as its representative for the purposes of voting in Plenary proceedings.

A Member shall join as a Participating or Observer Member as defined below:

- **Participating Members.** Participating Members are those stakeholders who actively participate in the Steering Group and the work of the Plenary, its Standing Committees, and Working Groups. The criteria for active participation such as attendance quotas or other measurable conduct shall be defined in the By-Laws. Participating Members shall have a vote in all Plenary proceedings.
- **Observing Members.** Observing Members are those stakeholders who do not meet the criteria for active participation, but want to maintain a presence in the Steering Group. Observing Members may still contribute to the work of the Plenary, its Standing Committees, and Working Groups, but they shall not be permitted to vote in Plenary proceedings.

## **1.6. Organizational Structure**

The Steering Group shall be composed of two bodies: the Identity Ecosystem Plenary and the Identity Ecosystem Management Council. The Plenary and the Management Council shall be collectively responsible for achieving the Steering Groups objectives.

## **1.7. Establishment**

The NSTIC, which was signed by President Obama in April 2011, called for the establishment of a private sector-led steering group to administer the development and adoption of the Identity

Ecosystem Framework. The Steering Group receives its authority to operate from the active participation of its membership. .

### **1.7.1. Resources and Duration**

The Steering Group shall be initiated with the support of NIST. Following the initiation period, the Steering Group will transition to a self-sustaining organization. The Management Council shall be responsible for managing the Steering Group's resources and procuring services once the Steering Group is self-sustaining, as necessary..

## 2. Identity Ecosystem Plenary

Participation in the Plenary shall be open to all Members. The primary responsibilities of the Plenary shall be to review and recommend technical standards for adoption establish and maintain the procedures/policies that govern the Identity Ecosystem, develop, and establish accountability measures to promote broad adherence to these procedures, and facilitate the ongoing operation of the Steering Group. The Plenary will consist of Standing Committees, Working Groups, and individual members. The Participating Members (as defined in section 1.5 and in associated By-Laws) of the Plenary shall be responsible for voting on recommendations provided by the Standing Committees and Working Groups and will participate in elections for Management Council Delegates, Management Council Officers, and the Plenary Chair.

### 2.1.1. The Plenary Chair

The Plenary shall be headed by the Plenary Chair. The Chair shall be responsible for directing the actions, managing the votes, and providing general leadership to the Plenary. Nominees for this position shall be approved by the Nominations Committee and selected by simple majority vote of the Participating Members that comprise the Plenary.

### 2.1.2. Plenary Standing Committees

Standing Committees shall be responsible for addressing and coordinating ongoing/permanent issues. Standing Committees shall produce their own charters and voting procedures which shall be approved by the Management Council. Additional measures may be taken by the Management Council to provide balanced and experienced representation on the Standing Committees. All recommendations proposed by the Committees shall be reviewed and approved by the Privacy Standing Committee prior to submission to the Plenary for approval.

The designated Standing Committees shall be:

- **Policy Coordination Committee.** The Policy Coordination Committee is responsible for coordinating policies to facilitate and promote the establishment of the Identity Ecosystem and the rules for participation.
- **Standards Coordination Committee.** The Standards Coordination Committee is responsible for coordinating, reviewing, and recommending the adoption of technical standards to facilitate interoperability within the Identity Ecosystem.
- **Accreditation Coordination Committee.** The Accreditation Coordination Committee is responsible for coordinating accreditation requirements for Identity Ecosystem participants.
- **Privacy Coordination Committee.** The Privacy Coordination Committee is responsible for seeing that other Committees' and Working Groups' work products adhere to the Privacy-enhancing and Voluntary Guiding Principle. To that end, this group should have a "gatekeeper" function; meaning no recommendations on policies, standards or other work products should be reviewed or approved by the Plenary unless first approved by the Privacy Coordination Committee. This committee should be staffed by individuals with extensive experience in the privacy field, and comprising a balance of viewpoints across a spectrum of experience, including advocacy organizations and the private sector.
- **Nominations Committee.** The Nominations Committee is responsible for evaluating candidate qualifications to serve as the Chair on the Plenary and Management Council or as a Delegate (Stakeholder group and At-Large). Selection criteria outlined in this Charter will

enable the selection of persons that can work for the welfare of the Identity Ecosystem as a whole, while minimizing self-interested conduct that could hinder the effectiveness and legitimacy of the Steering Group.

The Management Council may establish more Standing Committees as necessary to accomplish the work of the Steering Group.

### **2.1.3. Plenary Working Groups**

Members shall establish domain expert Working Groups as necessary to accomplish the work of the Steering Group. Working Groups may be proposed by the Plenary or the Management Council and shall be officially established by the Management Council. Participation in and meetings of the Plenary Working Groups shall be open to Participating and Observing Members; however, only Participating Members may vote on work products and recommendations.

Working Groups shall produce their own charters and voting procedures which shall be approved by the Management Council. Based on their work, Working Groups may propose recommendations and work products for consideration by the Plenary. All recommendations proposed by the Working Groups shall be reviewed and approved by the Privacy Standing Committee prior to submission to the Plenary for approval.

The following Working Groups shall be established by the Plenary and Management Council:

- **Usability and Accessibility Working Group.** This working group is responsible for evaluating technologies and identity solutions within the Identity Ecosystem to confirm that they are easy-to-use and accessible for all potential users, in accordance with the NSTIC Guiding Principles.
- **Security Working Group.** This working group is responsible for evaluating technologies and identity solutions within the Identity Ecosystem to confirm that they meet applicable requirements for confidentiality, integrity, and availability, and are capable of timely restoration after any disruption. The work of this group should be conducted in accordance with the NSTIC Guiding Principle for the security and resilience of identity solutions.
- **International Coordination Working Group.** This working group is Responsible for reviewing and, where appropriate, coordinating alignment with similar international identity standards and policies.

Additional Working Groups may be established by the Management Council or the Plenary as necessary to accomplish the work of the Steering Group.

### 3. Identity Ecosystem Management Council

The Management Council shall provide guidance to the Plenary on the broad objectives envisioned by the Strategy; produce workplans to prioritize work items and monitor progress; procure necessary resources; and ensure that Steering Group work activities align with the NSTIC Guiding Principles and Goals.

All recommendations from the Plenary Working Groups and Standing Committees shall be voted on by the stakeholder group delegates elected to the Management Council. The voting process will be structured and defined in the Steering Group By-Laws established during the initial meeting of the Steering Group. The Management Council shall also be the final ratification authority in the Steering Group.

#### 3.1. Management Council Composition

The Management Council shall be composed of 14 delegates, who are elected from the stakeholder groups and two at-large delegates. The Management Council may include additional stakeholder groups at any time as necessary.

In addition to Management Council Delegates, the Management Council shall have three (3) officers:

- **The Chair:** This position shall provide general leadership to the Management Council; oversee votes, and direct meetings of the Management Council. The Chair shall be a non-voting officer.
- **The Vice-Chair:** This position shall assist the Steering Group in maintaining alignment with NSTIC objectives and the NSTIC Guiding Principles. The Vice-Chair shall be a non-voting officer.
- **The Ombudsman:** This position shall be responsible for upholding the NSTIC Guiding Principles and Steering Group charter, representing and advocating for consumers or other individuals and underrepresented groups, safeguarding against individual stakeholder groups exerting excessive influence, monitoring and reporting on Management Council activities, managing grievances from the Plenary, and facilitating public comment and citizen outreach. The Ombudsman shall be a non-voting officer.

#### 3.2. Management Council Selection

The Management Council Delegates and Officers shall be selected through the following processes:

- **Delegates:** Management Council Delegates shall be selected through a general election held within each Stakeholder Group represented in the Plenary. The nomination of each candidate for the election will be approved by the Nomination Committee.
- **At-Large Delegates:** The election or selection process of At-Large Delegates shall be determined by the Steering Group during its initial meetings, as with all Management Council Delegates nominees shall be approved by the Nominations Committee.
- **Chair:** The Chair of the Management Council shall be selected through a general election of the Identity Ecosystem Plenary. The nomination of each candidate for election shall be approved by the Nominations Committee.
- **Vice-Chair:** This position shall be filled by the Director of the NSTIC National Program Office



- **Ombudsman:** This position shall be provided by the Secretariat. The criteria for selection shall be established by the Management Council.

Management Council positions, selections, elections, and appointments shall be conducted in accordance with by-laws created by the Steering Group during its initial meetings.

### 3.2.1. Delegate Selection Criteria

The Management Council Delegates (Stakeholder Group and At-Large) shall be selected in accordance with the following criteria:

- **Visionary Capability:** Delegates shall be capable of understanding and contributing to the multi-disciplinary aspects of the Identity Ecosystem and the specific goals of the Strategy.
- **Team Effectiveness:** Delegates shall be capable of working effectively as a team within the scope of the Management Council.
- **Outreach:** Delegates shall be able to clearly communicate the actions of the Management Council to their individual Stakeholder Group to facilitate consensus building and support the work of the Steering Group.
- **Expertise:** Delegates shall be recognized experts in their fields of endeavor.
- **Commitment:** Delegates shall be able to commit to contribute sufficient time and effort to accomplish Management Council activities.

### 3.2.2. Stakeholders

For the purposes of Management Council Delegate selections Members shall self-identify into one of the following 14 stakeholder groups:

- **Privacy & Civil Liberties.** This group focuses on the protection of individuals' privacy and civil liberties.
- **Usability & Human Factors.** This group focuses on technologies and solutions that are usable and incorporate the human, cognitive, and social properties unique to the characteristics of humans.
- **Consumer Advocates.** This group focuses on addressing the interests and accessibility of consumers and other individual end-user populations.
- **U.S. Federal Government.** This group focuses on the interests of the departments and agencies that comprise the U.S. Federal Government. Under its various forms and component programs, the government acts as an identity provider, attribute provider, and relying party. This group's Management Council Delegate will be responsible for advocating for the Federal Government as a Stakeholder; unlike the Vice-Chair who advocates on behalf of the NSTIC itself.
- **U.S. State, Local, Tribal, and Territorial Government.** This group focuses on the interests of the various state, local, tribal, and territorial governments that exist within the U.S.
- **Research, Development & Innovation.** This group focuses on research, teaching, and technology development in support of the Identity Ecosystem.
- **Identity & Attribute Providers.** This group focuses on the processes and technologies associated with establishing, managing, and securing digital identities and attributes.

- **Interoperability.** This group focuses on supporting interoperability within the Identity Ecosystem, inclusive of Trust Framework Providers and standards development organizations.
- **Information Technology (IT) Infrastructure.** This group focuses on IT infrastructure relevant to the functioning of the Identity Ecosystem, inclusive of different types of communications and network traffic, as well as virtual and distributed functions that produce and provide hardware, software, and IT systems and services.
- **Regulated Industries.** This group focuses on industries covered by sector-specific regulations that may be affected by the development of the Identity Ecosystem Framework.
- **Small Business & Entrepreneurs.** This group focuses on the impact of the development of the Identity Ecosystem Framework on small businesses and individual business owners/operators.
- **Security.** This group focuses on IT security services that support the confidentiality, integrity, and availability of identity solutions
- **Relying Parties.** This group focuses on transaction decisions based upon receipt, validation, and acceptance of an entity's authenticated credential(s) and identity attributes.
- **Unaffiliated Individuals.** This group consists of any individual who does not self-identify into one of the other stakeholder groups.

The Steering Group shall periodically review the list of designated stakeholder groups to confirm that it accurately reflects the broad array of Identity Ecosystem stakeholders and provides balanced representation for all parties. The Steering Group may add, modify, remove, or otherwise alter the stakeholder groups as it deems necessary.

## **4. Secretariat**

The Secretariat shall serve as the administrative body of the Steering Group. In this role, the Secretariat shall manage the internal operations of the Steering Group to include human and financial resources, meeting coordination, communications, and material support and interaction with external organizations. The Secretariat shall be responsible for maintaining transparency, openness, and alignment with the Guiding Principles in all Steering Group operations. The Secretariat shall appoint an individual to act as the Identity Ecosystem's Ombudsman.