THE CENTER FOR IDENTITY
THE UNIVERSITY OF TEXAS AT AUSTIN

Center for Identity Response to the National Strategy for Trusted Identities in Cyberspace (NSTIC) Notice of Inquiry (NOI)

Submitted by
Center for Identity
at
The University of Texas

Suzanne Barber
Director
sbarber@identity.utexas.edu

Norm Willox
Chairman, Board of Directors
nwillox@identity.utexas.edu

Center for Identity
Response to the National Strategy for Trusted Identities in Cyberspace (NSTIC) Notice of Inquiry (NOI)

Submitted by
Center for Identity
at
The University of Texas

This document describes governance models and values for a governance body to administer the processes for policy and standards adoption for the Identity Ecosystem Framework in accordance with the National Strategy for Trusted Identities in Cyberspace (NSTIC or "Strategy").

1. Key Values for the NSTIC Steering Group and its Host Organizational Partner

The *National Strategy for Trusted Identities in Cyberspace* (NSTIC or Strategy) charts a course for the public and private sector to collaborate in order to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions [1].

The NSTIC requires a governance organization to administer the process of policy and standards adoption for the Identity Ecosystem Framework in accordance with the NSTIC Strategy.

The NSTIC governance process (and ultimately the NSTIC Steering Group) requires the following key features:

- **Industry-led** – The private sector must lead the discussion because the private sector will implement the NSTIC Identity EcoSystem solutions and those solutions must interoperate with many existing solutions and standards. [1]
- **Unbiased** – The organization hosting the NSTIC Steering Group must have no vested interests in the outcomes.
- **Inclusive** – All the stakeholders of the Identity Ecosystem must be included.
- **Knowledge-intensive** – The best minds must be assembled to survey options and explore solutions on behalf of the industry-led decision-making body.

[1] National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy, April 2011.

- **Education**al – Dissemination of results and standards through focused education is vital for adoption of the NSTIC Strategy.
- **Accessible** – All key stakeholders must have access to the decision-making process, the results and the education.
- **Experienced** – The critical nature of the NSTIC Strategy, as well as the multiplicity of stakeholder interests will demand participation by topic-matter veterans having expertise in both establishing and operating a consensus-based decision-making consortium.
- **Fidelity to the spirit and implementation of the charge set forth by President Obama's Cybersecurity Policy Review** – "The Federal Government—in collaboration with industry and the civil liberties and privacy communities—should build a cybersecurity-based identity management vision and strategy for the Nation that considers an array of approaches, including privacy-enhancing technologies. The Federal Government must interact with citizens through myriad information, services, and benefit programs and thus has an interest in the protection of the public's private information as well "[2]

In order to rapidly stand up an NSTIC Steering Group, NSTIC should select a host organizational partner that (1) is aligned with the NSTIC mission; (2) can provide a robust administrative infrastructure capable of satisfying the requirements mentioned above, (3) possesses or can access very high quality research, development, and educational capabilities in all disciplines operating in the identity management and security environment.

Possibly most importantly, an organizational partner should excel with respect to all requirements set forth for the NSTIC governance process and the NSTIC Steering Group.

- **Industry-led** – A host organizational partner should be a public-private partnership through which industry offers valued leadership.
- **Unbiased** – A host organizational partner should offer an unbiased trusted environment where industry, government, non-profits and academia can collaborate to build the critical knowledge, standards and solutions for trusted transactions in cyberspace.
- **Inclusive** – A host organizational partner should be driven by the premise that trusted identities are required for trusted transactions everywhere. This would enable the Steering Group to bring together the needed research disciplines (policy, technology, law, business) and multiple enterprise sectors (energy, healthcare, financial services, commerce, government, law enforcement, and defense).

[2] "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure " The White House May 2009, p 33 Web 2 Jun 2010 http://www whitehouse gov/assets/documents/Cyberspace_Policy_Review_final pdf

- **Knowledge-intensive** – A host organizational partner should provide an environment that encourages the nation's thought leaders to share and develop knowledge that will lead to a trusted and secure cyberspace for our businesses, government and citizens for years to come.
- **Accessible** – A host organizational partner should provide an open environment for NSTIC collaborations with the capability to operate NSTIC offices across the U.S.; further, the host organizational partner should be able to provide the facilities and resources to allow all NSTIC partners to conveniently meet and work to make efficient and rapid progress on their mission. Lastly, the fast-host organizational partner should be able to develop and implement an information dissemination plan to allow all interested and affected industries to provide input and receive the latest progress and results from the NSTIC Steering Group.
- **Experienced** – A host organizational partner should have relationships with industry, government, academia, and non-profit partners who bring a wealth of experience vital for the NSTIC Strategy. Understanding past experiences as well as the possibilities for the future would provide well-informed, forward-looking resources for the NSTIC Steering Group.
- **Fidelity to the spirit and implementation of the charge set forth by President Obama's Cybersecurity Policy Review.** A host organizational partner should understand the uncompromising requirement to maximize the appropriate privacy and security in cyber-transactions.

2. Mantras of the NSTIC Steering Group (and its host)

The NSTIC Steering Group mission and structure must be directed by assumptions and guidance provided by the vision for the Identity Ecosystem, NSTIC Strategy's Guiding Principles, components for the Identity System Ecosystem Framework, the Fair Information Practice Principles (FIPPs) and the assurance that all participation in the Identity Ecosystem will be voluntary.

Specifically, the NSTIC Steering Group governance organization assisted by its host organization must:

- Create a NSTIC Steering Group framework of strategic goals and metrics in direct support of the NSTIC Strategy and Guiding Principles.

- Support and institutionalize proactive mechanisms for the NSTIC Steering Group to continually evolve NSTIC policy and planning.

- Support initiation and execution of a NSTIC Steering Group governance structure that supports the diversity of stakeholders within and between sectors as well as the realities of the range of transactions and operations.

2.1. Vital features of a successful model for the NSTIC Steering Group organization structure

There are many models of governance that perform some of the wide range of functions needed to formulate and administer the Identity Ecosystem Framework. While not all of these functions are unique to the Steering Group, few examples of governance cover the same breadth of the technical, policy and economic landscape as the Identity Ecosystem Framework. The NSITC Steering Group, therefore, has a greater risk of either being too small to serve its purpose, or too large to govern effectively.

There is a full spectrum of affected economic sectors, some of which are highly-regulated, while still others are unregulated. The NSTIC Steering Group will need to simultaneously integrate the Identity Ecosystem Framework with regulatory requirements faced by firms in a variety of industry sectors. At the same time, the NSTIC Steering Group needs to consider and represent the interest of the broader public in security and privacy. It is imperative to find a working structure that accomplishes all these needs.

The UT Center for Identity offers the following responses to questions posed in the NSTIC Notice of Inquiry (NOI).

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

The Steering Group governance model must be organized for service to…

- Represented enterprise sectors and their direct participation to ensure engaged stakeholders;
- The Guiding Principles; and,
- Stakeholders that provide or use solutions within the Identity Ecosystem.

Two particularly difficult issues that are not specifically addressed, but that must be within a consortium activity are:

1) Assurance of influencing and performing work that is strictly pre-competitive; and,
2) Assurance that the consortium does not select solutions, or create influence so as to inadvertently "crown winners" in the private sector.

A primary directive by the Steering Group's executive board must be that an even playing field will be provided to all participants and only pre-competitive work will be performed.

2.1.2. To what extent does the Steering Group need to support different sectors differently?

The Steering Group should be organized and governed so as to allow inclusion of and uniformly equal (but perhaps weighted) support for all enterprise sectors. When a need arises for supporting different sectors differently, it will likely be characterized by needs connected to…

- Confidentiality and secrecy (e.g., law enforcement and national security),
- Commercially proprietary intellectual property (e.g., commercially competitive information/property),
- Regulated versus non-regulated enterprise sectors (e.g., practices and standards imposed by the force of law versus practices and standards that are commercially advantageous), and
- Civil liberties (e.g., assuring the appearance and fact of safe-guarding individual liberties).

The Steering Group should be sensitive to these differences and organized to support them to every extent possible.

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

The NSTIC Steering Group must include the appropriate industry and government regulators to avoid conflict with rules set for both industry and government participants in the Identity Ecosystem (e.g., Federal Trade Commission).

Additionally, the proposed NSTIC Steering Group must be charged to proactively search for and identify applicable regulations that the NSTIC Steering Group must consider and incorporate into all work products.

To mitigate the potential risks, the NSTIC Steering Group must provide a collaborative framework to allow safe harbor for private interests to engage.

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

If regulators and/or regulated participants present compelling arguments in an open exchange of ideas about approaches used in their industries that are fully supported by the guiding principles, then "pull-through" should be noted and not feared. If the regulation is working and not oppressive, and can be adapted to the unregulated industry without loss of those positive attributes, then it should be considered effective and useful. The fundamental assumption for "pull-through" regulation should be "by the consent of the regulated" if applied to a new set of unregulated participants.

2.1.5. What are the most important characteristics (e.g., standards and technical capabilities, rulemaking authority, representational structure of the Steering Group? How should the government be involved in the Steering Group at steady state? What are the advantages and disadvantages of different levels of government involvement?

The single most important organizational characteristic of the Steering Group is the even-handedness of the representational structure. All stakeholders must be represented, directly engaged, and that representation and engagement must be visible. Failure to do so will immediately appear to favor someone: government over the individual; the financial industry over the individual; the energy industry over the environmental protection interests, etc.

From another view, it is essential to have full participation in the Steering Group by the academic disciplines and identity ecosystem expertise needed to develop and deploy solutions that successfully resolve all aspects of the grand challenges represented as Guiding Principles. Full engagement of experts from business, government, and academia will be needed to fill the gaps, push the envelope, embrace solutions, and ultimately, realize the ambitious goals of the NSTIC Strategy.

Government should be involved with the Steering Group as a "relying" customer, a funding supporter, an expertise provider, and protector – by providing safe-harbor protection to enable open and frank discussions without fear of legal reprisal. Government should also have a loud voice in that the value and volume of governmental identity related transactions are very large. That said, government should be very careful about imposing restrictive public policy upon the Identity Ecosystem due to the personal and emotional nature of identity and its transaction. At steady state, the government's involvement with the Steering Group should be primarily as a major

stakeholder and customer for solutions. The government's role as a funding source should probably decrease as the Steering Group or its derivative matures.

2.2. NSTIC Steering Group initiation must "begin well" to establish an organization structure and stakeholder representation that can scale to success.

This concept of a strong beginning for the Steering Group is critical for success. Participants will be drawn to an organization that possesses directly engaged members, membership "skin-in-the-game," resources to support the mission, deep and broad research and development capabilities, fully functional and expandable facilities, demonstrated influence on standards and policy, and a capable education and outreach function. The organization much provide noteworthy product on a quarterly basis, presented in high-profile international meetings. Demonstrated capability and success in these areas will provide the critical mass that will in turn attract other participants.

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

Functioning of the NSTIC Steering Group should depend on a scope defined solely by its mission and strategic plan. The NSTIC Steering Group authority must be scoped by the authorizing government agency, NIST, in accordance with the President's executive order. In order to achieve the stated mission and strategic plan, the method by which the NSTIC Steering Group is initiated must not influence the authority that the Group requires, both at its initiation and in its future.

Many existing for-profit and non-profit organizations have established missions, some of which may align reasonably well with the NSTIC mission. While these missions may also be supportive of the NSTIC Steering Group, these missions could limit or distract the functioning and authority of the NSTIC Steering group. There are significant advantages to including all the stakeholders represented by for-profit, not-for-profit government agencies, and non-profits in the NSTIC Steering Group initiation. Most importantly, all of the voices should be considered and included appropriately. The following table outlines the disadvantages to exclusively employing one of these existing organizational structures to initiate the NSTIC Steering Group.

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

The government's endorsement of the effort as both a funding agent and eventual consumer of derivative commercial product is extremely important to early success. This endorsement attracts private-sector members, and is important (if not critical) to initial phase success. As mentioned above, the government can provide legal protection against antitrust accusations or actions through safe-harbor designations for the Group. Governmental agencies also bring extensive experience (FICAM), expertise, and empirical experimental and test data that are not available in the private sector. Finally, the government can provide policy support that might be needed to "jump start" adherence to Steering Group recommendations and critical standards.

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

Self-regulated commercial enterprises with government oversight and partnership tend to be trusted in the United States. The NSTIC Guiding Principles will flourish under a blended model incorporating public-private partnership having defined roles, responsibilities and authority. The NSTIC Guiding Principles must be the driving forces from day one. There is a Japanese saying, "All is well that begins well." There is another wisdom that similarly expresses the importance of starting well: "Begun well, half done." The NSTIC Steering Group should start with the values, mission and structure of stakeholder inclusion that most closely reflects its target end state.

Certain methods for initiating the NSTIC Steering Group will introduce greater risks to the Guiding Principles.

- If the NSTIC Steering Group is exclusively led by and comprised of commercial interests at this initiation phase, noteworthy risks include:
    - The strongest and most influential enterprises could dominate the discussion and influence solutions toward their proprietary offerings. It's the "big dog on the porch" problem. A strong, unbiased, egalitarian governance structure can control this.
    - Many people do not trust the profit motive and would be suspicious of an organization governed by for-profit enterprises without public or non-profit oversight and possibly controls.

- If the NSTIC Steering Group is exclusively led by and comprised of government agencies at this initiation phase, noteworthy considerations must address willingness of government to provide "just enough" leadership without becoming a dominating, regulating, and perhaps stifling force.

A "blended" model is required. The NSTIC Steering Group must be led by self-regulated commercial enterprises with strategic government oversight.

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

The NSTIC Steering Group should be comprised of self-regulated commercial enterprises with government oversight and partnership. The Government's role should be clearly established and consistent from day one in order to ensure that the organization is aligned with and prepared to advance the NSTIC mission from the outset.

The government recognizes a critical role for the NSTIC Steering Group, and that role should be uniform from the initiation of the organization and remain the same throughout the NSTIC program lifecycle. The government is a major stakeholder, offering…

- Funding for early stage operations;
- Major stakeholder requirements and metrics for success;
- Opportunities to serve as an early adopter in order to transition technology to the public sector for rapid commercialization; and
- Policy and regulation recommendations to promote or limit outcomes in the best interests of citizens and the nation.

It should be recognized that "Government" is a broad term that should be further defined. Government agencies serve as identity providers, attribute providers or relying parties in cyberspace to include but not be limited to: NIST, State Department, DHS, US Secret Service, FBI, Veterans Affairs, etc.

2.3. A host organizational partner must put extreme value on ensuring that stakeholders are represented in the Steering Group

A productive NSTIC Steering Group governance structure will embrace a diversity of sectors and disciplines, and ground an understanding of current and predicted cyber transactions and operations. For a national cyberspace that impacts all aspects of our Nation's infrastructure, the NSTIC Strategy must engage all of its stakeholders that are directly engaged and representing industry, government, law enforcement, academia, privacy advocates, and non-profits representing vital missions for industry and the consumer.

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

The Steering Group composition should be representative of stakeholders from multiple sectors. The NIST Smart Grid Advisory Committee represents an example of representatives for key sectors and stakeholders.

2.3.2. How should interested entities that do not directly participate in the Identity Ecosystem receive representation in the Steering Group?

All stakeholder interests should be represented via their own organization's participation, or through an organization that shares their interests in a given sector.

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

Government and Law Enforcement are critical sectors at the executive governance level with invited representation. Non-Federal governments can be represented as an enterprise sector, as can foreign governments.

2.4. International

Given the global nature of online commerce, the Identity Ecosystem cannot be isolated from internationally available online services and their identity solutions. Without compromising the Guiding Principles of the Strategy, the public and private sectors will strive to enable international interoperability. In order for the United States to benefit from other nations' best practices and achieve international interoperability, the U.S. public and private sectors must be active participants in international technical and policy forums.

No single entity, including the Federal government, can effectively participate in every international standards effort. The private sector is already involved in many international standards initiatives; ultimately, then, the international integration of the Identity Ecosystem will depend in great part upon private sector leadership.

2.4.1. On what international entities should the Steering Group focus its attention and activities?

The international entities of most interest to this endeavor are arguably international standards groups and private sector enterprises that develop useful hardware and software technologies and solutions. Further, the development of increased support from international law enforcement organizations should be encouraged.

2.4.2. How should the Steering Group maximize the Identity Ecosystem's interoperability internationally?

International interoperability should be assured through representation on the executive level board, and resulting integration with international standards and law enforcement agencies. Also, the executive level board should encourage international support for direct inquires and requests from the Steering Group's stakeholders.

2.4.3. What is the Federal government's role in promoting international cooperation within the Identity Ecosystem?

Beyond ideas provided above, the federal government should establish and enforce State Department limitations of participation by OFAC nations, and assist in inviting and encouraging participation by trading partners holding "most favored" status.

3. About the Center for Identity

The mission of the Center for Identity at The University of Texas is to deliver the highest quality identity management discoveries, applications, education and outreach available. The research and education endeavors of the Center break new ground to prepare its members to anticipate and mitigate current and future identity threats. The Center serves as a state and national treasure to meet near term research, application, and education needs while offering leadership, vision, and solutions for the future.

The Center offers research innovations to uniquely define and protect the identities of people, organizations, and entities in both cyber and physical environments. From basic research to applied research, serving a wide range of industrial, government and defense applications, the Center will offer identity definitions, best practices, lifecycle management and technology to ensure its Partners and the nation remain ahead of the growing identity challenges. The Center will work specifically to identify and integrate the technological, legal, cultural, commercial, and public policy solutions required to translate identity management and protection research into deployed solutions.

Central to the mission of the Center are educational programs including short courses, seminars, certifications and degree programs to prepare working professionals, consumers, and new UT-Austin graduates to develop and implement the superior business processes, policies, and technologies to authenticate and safeguard identities throughout their organizations, their careers, and their lives.

The Center for Identity is an epicenter of identity solution excellence brought about by active collaborations to meet our community, business, state, and national identity challenges. The Center pairs the depth and breadth of knowledge and talent at The University of Texas with its Partners from industry, government, and academia to offer the best thinking and solutions available to enroll, authenticate, and protect identities everywhere. The Center provides an unbiased public service, delivering trusted information concerning identity threats and protection.

The Center for Identity is comprised of thought leaders from government, corporate, and academic organizations who share a common interest in research and education for meeting current and future identity management challenges impacting individuals, public safety, commerce, government programs, and national security. The Center's founding Partners are leaders from industry (Acxiom, FICO, Gemalto, IBM, ID Experts, InfoZen, Intersections, LexisNexis, SRA International, TransUnion, Visa), government agencies (FBI, Texas Department of Public Safety, US Department of Defense, US Marshals Service, US Secret Service), and non-profit organizations (Identity Theft Assistance Center (ITAC), Identity Theft Council, National Cyber Forensics Training Alliance (NCFTA), and TechAmerica).