Smart Card Alliance Response

NIST Notice of Inquiry: Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace

Docket No. 110524296-1289-02

July 21, 2011

The Smart Card Alliance is pleased to submit comments to NIST on the Notice of Inquiry (NOI), "Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace (NSTIC)," Docket No. 110524296-1289-02. The comments below include discussion of general principles that the Alliance believes NIST should follow in establishing NSTIC governance, followed by specific answers to the questions in the NOI.

The Smart Card Alliance is a not-for-profit, multi-industry association working to accelerate the acceptance of smart card technology. Members from our Identity Council collaborated to compile the comments below. The Identity Council is a cross-industry group of manufacturers, systems integrators and end users, focused on identity management and secure identity authentication.

The Smart Card Alliance appreciates the opportunity to provide input to NIST on the NSTIC governance model.

General Principles for the NSTIC Governance Model

General principles that should guide the NSTIC governance model are as follows:

- Governance should be driven by the private sector, not government. Government is a key stakeholder in the identity ecosystem and should participate as a stakeholder, rather than as the administrator.
- Funding is needed both during organization formation and in steady state. The government should consider providing seed funding during the formation phase. The steering group will need to define the business and funding models for maintaining the organization in steady state as one of its initial tasks.
- Organization members should work in peer relationships, with all members having an equal vote regardless of the size of the organization.
- Steering group processes should be deliberate, transparent and open to all members and to the public.
- Development of the organization should be in phases, with the Smart Grid initiative a useful model of how to accomplish the phased development.
- All stakeholders must be able to have a voice in the steering group, and the organization must make a conscious effort to include smaller organizations, consumers, privacy groups and end users.
- The steering group must be tasked to develop a sustainable funding model for the organization, with no special category of members or funding level required for representation on the steering group.
- The organization must be sensitive to international requirements and implement a structure that engages with the international community.

- Government involvement should be as a stakeholder and be structured to minimize the legal impact to the organization (e.g., involvement should be such so that FACA can be avoided).
- The organization focus should be to build on existing infrastructure and standards, developing action plans to address weaknesses.

Section 1. Structure of the Steering Group

Questions:

1.1. Given the Guiding Principles outlined in the Strategy, what should be the structure of the steering group? What structures can support the technical, policy, legal, and operational aspects of the Identity Ecosystem without stifling innovation?

The success or failure of NSTIC will rely on several factors. The overall governance structure of the steering group is one of the biggest key contributing factors; other factors will be such items as managing quality participation by as many interested parties as possible; being accessible to all; being fair and democratic; and having adequate sustainable funding.

Many organizations and associations today exist with a management board, organization officials and a substructure of working groups or committees that undertake the detailed operation of the organization and service to its membership. These organizations are generally governed by a set of executed bylaws, have membership criteria (such as common interests), and have a dues/funding structure. They also have auditable accounts and a democratic process for electing the organization's officers.

NSTIC can fit this organizational model with careful attention to the steering group composition and the regulation of its operation.

In the opinion of the Smart Card Alliance, it is important for the NSTIC steering group to be composed of two elements:

1. The administrative function.

    This function would be composed of resources dedicated to the sustainable operation, logistics and management of the entire NSTIC collective, providing direct support to the management function. The administration resources should be independent of any outside influence and not have a stake in the material content or output of NSTIC. The head of the administrative function would be represented on the management function and could act as the organization's spokesperson.

2. The management function.

    This function would define the bylaws and abide by them; set the mission and scope of the organization; set strategic objectives; and define a sub-structure of committees and working groups. This function would also be the decision maker for all organization output and would be the referee for policy questions and conflict.

The composition of the management function is critical. Unlike many organizations today, the NSTIC management function should be open to all potential stakeholders without any one member being allowed to dominate proceedings. For consideration, we suggest the management function be composed of organizations representing multiple members wherever possible – i.e., the management board would be composed of associations, organizations, and coalitions which have multiple members.

The management function membership should be open to both voting members and non-voting (observing) members. This would allow government (non-voting) presence and representation along with academia.

Commercial entities should be limited to membership in the management function through a trade organization, industry association or other similar structure.

By creating the steering group composition as outlined above, multi-member organizations (usually of like-minded/specialist members) can engage their memberships in providing skilled resources and quality input to the sub-structure of NSTIC, such as volunteers to work in committees on policy and technology.

1.2. Are there broad, multi-sector examples of governance structures that match the scale of the steering group? If so, what makes them successful or unsuccessful? What challenges do they face?

NSTIC presents unique challenges of representation to the steering group composition since it spans many sectors of potential involvement. The Smart Card Alliance has a record of success in maintaining both commercial and government membership in an organization dedicated to the mission of education on the use of smart cards in many applications. The organization has a dues-based, tiered membership level structure with an elected Board of Directors. Board officers are democratically elected from the top tier membership level and a permanent administrative/leadership resource is present to run the Smart Card Alliance operations. Bylaws are used to operate the organization fairly and legally. The Alliance substructure is composed of Board committees along with special interest groups, termed "Councils," which are open to all members and have elected Council officers. The role of the Councils is to work on deliverables relevant to their domain and provide value to others in the exchange of knowledge.

Broad public involvement is also important for successful adoption of new NSTIC standards and framework. The steering group could accomplish this through public outreach – by publishing open drafts and soliciting public comments (e.g., as the IETF does or as NIST did for the draft NSTIC framework).

1.3. Are there functions of the steering group listed in this Notice that should not be part of the steering group's activities? Please explain why they are not essential components of Identity Ecosystem Governance.

No comment.

1.4. 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?

For NSTIC to succeed, two aspects of the steering group require special attention – first, the initial formation and startup of the steering group, and second, the sustainability of the steering group.

The initial formation and startup should be completed as quickly as possible by establishing the administration function first, then gathering membership applications (and dues if deemed appropriate). Once the steering group composition is established by the administration function, bylaws should be defined and agreed upon, the substructure determined, and resources identified to work on the activities needed.

The sustainability of the steering group should be ensured with sufficient renewable funding from membership dues and/or government grants. Assignment of steering group membership positions should be, at a minimum, annual, with elections for any officer positions.

1.5. To what extent does the steering group need to support different sectors differently?

This should be done with care, ensuring government stakeholder inclusion and allowing for fair inclusion of commercial associations, interest groups and individuals. The critical aspect to ensure is maintaining the independence of the administrative function and not allowing any one entity to dominate the steering group.

The use of committees or working groups from the different sectors helps to engage the various sectors in the development and review of different aspects of their framework and standards.

1.6. 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?

Government participation is essential to ensure any policies are formulated correctly in terms of adoption by the NSTIC community and organizations that will use them for the ecosystem operation.

Public review and comment periods (that are held for a reasonable amount of time) will provide individuals from all sectors of society with the opportunity to submit written comments, arguments, data and views on any proposed rules.

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

The definition of policies relating to the guiding principles should be carefully constructed to ensure successful adoption by the ecosystem. Legal support would be necessary for interpreting these polices for any regulated participants.

By ensuring the participation of relevant industry and community groups, the risk is automatically mitigated.

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

The steering group should be composed of several specialist subgroups. These should at a minimum be (1) policy, (2) technology, (3) standards, and (4) compliance committees. The overseeing steering group should be the final arbiter and publish rules, policies, specifications and compliance requirements.

1.9. 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?

While government involvement in the steering group is essential and individual government employee participation would be helpful, there exists a concern that the organization could then be subject to FACA rules. The steering group must be independent of FACA. An alternative could be that government be represented on the steering group as permanent non-voting advisors to avoid FACA rules. The steering group must be independent of direct government input to ensure maintenance of NSTIC neutrality as a guiding principle.

Section 2. Steering Group Initiation

Questions:

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?

No comment

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 meaningful participation of stakeholders is critical to the success of the steering group. The government is one stakeholder with valuable and unique skills.

The involvement of the government in a supportive and advisory role during the initial creation of the group will help to make clear the scope and importance of the initiative.

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

See answer to 2.2. In addition, providing government funding during the initial phase can help while the steering group is formed and while it is defining the business model, full organization structure and the means to support the organization.

2.4. 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?

Stakeholder participation is based on the principles of transparency, accountability, and democratic participation in decision-making. An appointed steering group can represent great risk to these principles. Steering group positions must be filled by election of candidates selected from stakeholder groups.

Stakeholder representation could include those that:

- May have skills and information useful to decision-makers, planners, and implementers;
- Have a demonstrated and vested interest in the impact of the policies and plans on their organization, business or community;
- May need to implement changes as a result of the policies and plans;
- May need to "buy in" to the policies and plans in order for the policies and plans to be implemented successfully.

See the Smart Card Alliance discussion of stakeholder groups in question 3.1.

2.5. 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 initial government role should be to participate as a stakeholder in the definition of the steering group structure. The private sector is involved at the beginning of this process and, as a result, there isn't a need for a transitional organization.

Section 3. Representation of Stakeholders in the Steering Group

Questions:

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?

Given the diverse and extensive number of organizations involved in the identity ecosystem, one way to engage these organizations is by engaging the organizations they belong to as a group (i.e., in industry or trade associations). A number of industry organizations represent members of the identity ecosystem. At a high level, these organizations could represent:

- Identity Providers
- Attribute Providers
- Consumer, Privacy and Civil Liberty Organizations
- Communication and Information Technology Infrastructure Providers
- Software and Application Providers
- Certification and Education Organizations
- Academic and Research and Development Organizations
- Relying Parties (representing major industry sectors)
- Standards Development Organizations
- The United States Federal Government
- State, Local, Tribal and other Governments

The steering group should include the leadership and/or subject matter, policy and operational expertise of these organizations, including CIOs, CTOs, CSOs and CISSPs, among others. It should include individuals with experience in large-scale infrastructure and systems that support users in the millions. If the individuals participating on the steering group represent multiple organizations, then the representation of the steering group is more representative of the identity ecosystem as a whole. In addition, the steering group should leverage work groups and think tanks to address particular areas of interest and challenges in establishing an identity ecosystem that meets NSTIC's goals.

3.2. How should interested entities that do not directly participate in the Identity Ecosystem receive representation in the steering group?

The steering group should be fully transparent and open to public observation and public comment periods. It should maintain at-large seats for individuals who can provide leadership and expertise.

These interested entities and their representative individuals should express their interest, be involved in the NSTIC process, and be invited to participate as at-large members via a selection process to be determined. That being said, the nature of the "indirect" participation and the process by which "at large" members become part of the steering group needs further consideration.

3.3. What does balanced representation mean and how can it be achieved? What steps can be taken to guard against disproportionate influence over policy formulation?

Balanced participation means that representation on the steering group is spread across the stakeholders in the ecosystem outlined in question 3.1. Representatives should apply to be part of the steering group. The steering group should have a limit to the number of individuals from a particular firm/organization. In addition, the steering group should look to have members of both large and small organizations and for-profit and not-for-profit organizations, and also include a balance of providers and users. This can be achieved by allocating seats on the steering group to individuals that represent different components of the identity ecosystem. Besides wide representation across identity ecosystem stakeholders, a supermajority could be used in order to establish policy and guard against disproportionate influence.

3.4. Should there be a fee for representatives in the steering group? Are there appropriate tiered systems for fees that will prevent "pricing out" organizations, including individuals?

No. Organizations may pay a fee to be a member of the organization, but there should be no further fee to be on the steering group.

The steering group will require funding in order to operate. And while fees may provide some revenue, it is unlikely that they will provide sufficient funding during the initial phase. Fees, if they are put into place, should be structured so that the steering group does not discriminate against organizations based on size. Many organizations use tiered pricing in order to make participation open and the steering group should make it a policy to achieve this goal.

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

Other and multiple sources of funding can be used, besides or in addition to fees, to maintain the governance body. These can include:

- Federal funding
  - Positive – Provides ability to initiate the steering group without funding concerns
  - Positive – Provides an ability to engage the best possible organizations and individuals without a concern about ability to pay (e.g., option for "scholarships")
  - Negative – Current funding and budget environment
  - Negative – Possibly contrary to the concept of "industry-led"
- Sponsorships (unrelated to representation)
  - Positive – Provides an additional revenue source and improves the ability to have tiered fees
  - Negative – Could be seen as a potentially commercializing initiative
  - Negative – Requires administration

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

All members should have the same voting rights.

3.7. 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?

The Federal government may have an interim role while the steering group is being established in order to provide an initial governance capability. State, local, tribal, territorial and other governments represent one of the stakeholder organizations outlined in question 3.1 and could have representation on the steering group.

Section 4. International

Questions:

4.1. How should the structure of the steering group address international perspectives, standards, policies, best practices, etc?

The challenges and opportunities that the steering group is to address are not unique to the United States. It will therefore be critical for the steering group to include international perspectives, standards, policies, and best practices. Further mapping and research of the related activities in the different regions of the world (e.g., EU, Asia, South and Central America) and organizations (e.g., UN, EU, ISO, ITU, NATO) will need to take place to determine the importance of the different international activities to NSTIC and the steering group and the approach to address each of them.

Based on the research, the steering group can make informed decisions on how to utilize the international perspectives. It is encouraged that every steering group discussion and decision have a review of relevant international initiatives and perspectives as part of the analysis.

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

Both industry and government are involved in other international entities – e.g., standards organizations and trade organizations. An analysis needs to be performed to identify all relevant international entities and the U.S. government and/or U.S. private sector companies that are/may be involved with these international entities.

There is a defined role for the U.S. government in participating with other international entities, specifically foreign governments. The U.S. government should therefore assign clear government leads for coordination with other foreign governments and provide sufficient support in maintaining these relationships to ensure that appropriate information is received in support of NSTIC activities.

Based on this analysis, the steering group can determine prioritized relationships and determine possible coordination approaches. These approaches can include leveraging existing U.S. memberships, assigning representation, having membership that allows for the receipt of documentation, and requesting U.S. government participation. Funding should be made available to support coordination with international entities.

The steering group should also consider the criticality for the U.S. to be represented in specific international entities (e.g., ISO) when topics and technology are being addressed that have an impact on what the U.S. and NSTIC are trying to achieve.

In addition, the Smart Card Alliance believes that international entities may choose to be directly involved in the NSTIC process through any of a number of activities that are available as a result of it being an open group seeking best practices.

4.3. On what international entities should the steering group focus its attention and activities?

There are numerous international entities that are active in the field of identity management and cyberspace. As mentioned previously, an analysis should be performed to determine all of the different legitimate activities by international entities that are of relevance to NSTIC. In certain instances there is a clear role for the U.S. government in being represented and assisting in supporting NSTIC activities.

The following international entities are examples of organizations that could be considered:

- UN
- EU (Council, Commission and Parliament)
- NATO
- INTERPOL
- ISO
- ITU

4.4. How should the steering group maximize the Identity Ecosystem's interoperability internationally?

Where possible the steering group should support the development of open, international standards, agreements and initiatives (e.g., pilots) to achieve international interoperability.

Cyberspace is seen as a global environment and requires close cooperation. A good example is the challenge faced by the international community in determining whether a cyber-attack is an act of war and the approach to address an attack. Governments and industry should work closely together to ensure that cyber-attacks against commerce be addressed in coordination. The increased coordination among different CERT organizations globally (there are some 250 independent CERT organizations globally) is one key component to consider for the steering group.

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

The Federal government has an important role and responsibility in promoting international cooperation and should actively be engaged with the steering group and NSTIC to determine how to utilize international cooperation and to set priority in promoting international cooperation within the identity ecosystem.

Consideration should be given to assigning an official government liaison to NSTIC to ensure coordination among the different Federal agencies involved (e.g., DoS, DHS, DoC, DoD, DoJ), as well as with the White House and the intelligence and cybersecurity communities, and to develop a unified strategy and approach in support of NSTIC.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.

Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.