PayPal™
Information **Risk Management**
Internet Standards and Governance

July 22, 2011

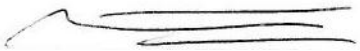
Patrick Gallagher
Under Secretary of Commerce for Standards and Technology
National Institute of Standards and Technology
c/o Annie Sokol, 100 Bureau Drive, Mailstop 8930
Gaithersburg, MD 20899

Dear Patrick et al.,

Thank you for the opportunity to review and respond to your notice of inquiry regarding models for a governance structure for the National Strategy for Trusted Identities in Cyberspace. We have attempted to provide constructive and clear guidance for how to position and structure the NSTIC Steering Group in a many most likely to result in success. Feel free to call upon us to clarify or discuss any of the recommendations we have provided herein.

You will find the text of our contribution called out in blue courier font in context of the complete notice of inquiry provided below.

Respectfully,



Michael Barrett
CISO, VP Information Risk Management
PayPal Inc, an eBay company

2211 N. FIRST STREET / SAN JOSE, CA 95131 / PHONE (408) 967-XXXX / FAX (408) 967-XXXX

WWW.PAYPAL.COM

Billing Code 3510-13

DEPARTMENT OF COMMERCE

Office of the Secretary

National Institute of Standards and Technology

[Docket No. 110524296-1289-02]

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

AGENCY: Office of the Secretary, U.S. Department of Commerce and National Institute of Standards and Technology, U.S. Department of Commerce.

ACTION: Notice of Inquiry.

SUMMARY: The Department of Commerce (Department) is conducting a comprehensive review of governance models 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"). The Strategy refers to this governance body as the "steering group." The Department seeks public comment from all stakeholders, including the commercial, academic and civil society sectors, and consumer and privacy advocates on potential models, in the form of recommendations

and key assumptions in the formation and structure of the steering group. The Department seeks to learn and understand approaches for: 1) the structure and functions of a persistent and sustainable private sector-led steering group and 2) the initial establishment of the steering group. This Notice specifically seeks comment on the structures and processes for Identity Ecosystem governance. This Notice does not solicit comments or advice on the policies that will be chosen by the steering group or specific issues such as accreditation or trustmark schemes, which will be considered by the steering group at a later date. Responses to this Notice will serve only as input for a Departmental report of government recommendations for establishing the NSTIC steering group.

DATES**:** Comments are due on or before July 22, 2011.

ADDRESSES**:** Written comments may be submitted by mail to the National Institute of Standards and Technology, c/o Annie Sokol, 100 Bureau Drive, Mailstop 8930, Gaithersburg, MD 20899. Electronic comments may be sent to *NSTICnoi@nist.gov*. Electronic submissions may be in any of the following formats: HTML, ASCII, Word, rtf, or PDF. Paper submissions should include a compact disc (CD). CDs should be labeled with the name and organizational affiliation of the filer and the name of the word processing program used to create the document. Comments will be posted at www.nist.gov/nstic. The Strategy is available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf. The NIST website for NSTIC and its implementation is available at www.nist.gov/nstic.

FOR FURTHER INFORMATION CONTACT**:** For questions about this Notice contact: Annie Sokol, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau Drive, Mailstop 8930, Gaithersburg, MD 20899, telephone (301) 975-2006; e-mail *nsticnoi@nist.gov.* Please direct media inquires to the Director of NIST's Office of Public Affairs, gail.porter@nist.gov.

SUPPLEMENTARY INFORMATION**:** Recognizing the vital importance of cyberspace to U.S. innovation, prosperity, education and political and cultural life, and the need for a trusted and resilient information and communications infrastructure, the Administration released the Cyberspace Policy Review in May 2009. Included in this review was a near-term action to "build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation." The completion of this action is the National Strategy for Trusted Identities in Cyberspace (NSTIC or "Strategy"), released in April 2011. The Strategy called for the creation of a National Program Office to be hosted at the Department of Commerce, as part of its ongoing cybersecurity and identity management activities. The Department intends to leverage the expertise present across many bureaus at the Department and across the U.S. Government, as well as experts in industry, academia, governments at all levels, communities of interest (including privacy, civil liberties, and consumer advocates), and the general public, through a series of inquiries and public workshops. This Notice of Inquiry is a continuation of the Administration's effort, and its goal is to explore the establishment and structure of governance models. The Department may explore additional areas in the future.

Background: This Notice reflects the initial steps of the Strategy's implementation as they relate to the Department's ongoing cyber security and identity management activities. Specifically, the Strategy calls for a "steering group" to administer the process for policy and standards development for the Identity Ecosystem Framework in accordance with the Strategy's Guiding Principles. The Identity Ecosystem is an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities and the digital identities of devices. The Identity Ecosystem Framework is the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that govern the Identity Ecosystem.

The Strategy's four Guiding Principles specify that identity solutions must be: privacy-enhancing and voluntary, secure and resilient, interoperable, and cost-effective and easy to use. The establishment of this steering group will be an essential component of achieving a successful implementation of the Strategy; a persistent and sustainable private sector-led steering group will maintain the rules of participating in the Identity Ecosystem, develop and establish accountability measures to promote broad adherence to these rules, and foster the evolution of the Identity Ecosystem to match the evolution of cyberspace itself.

The government's role in implementing the Strategy includes advocating for and protecting individuals; supporting the private sector's development and adoption of the Identity Ecosystem; partnering with the private sector to ensure that the Identity Ecosystem is sufficiently interoperable, secure and privacy enhancing; and being an early adopter of both Identity Ecosystem technologies and policies. In this role, the government must partner with

the private sector to convene a wide variety of stakeholders to facilitate consensus, with a goal of ensuring that the Strategy's four Guiding Principles are achieved. The government has an interest in promoting the rapid development of a steering group capable of, and equally committed to, upholding the Strategy's Guiding Principles.

The Strategy calls for the development of a steering group that will bring together representatives of all of the interested stakeholders to ensure that the Identity Ecosystem Framework upholds the Guiding Principles by providing a minimum baseline of privacy, security, and interoperability through standards and policies—without creating unnecessary barriers to market entry. To that end, the steering group will administer the process for the adoption of policy and technical standards, set milestones and measure progress against them, and ensure that accreditation authorities validate participants' adherence to the requirements of the Identity Ecosystem Framework.

With this outcome in mind, the government seeks comment on the establishment and structure of a steering group that can successfully complete the above stated goals and objectives and, ultimately, achieve the Strategy's vision that "individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."

Contribution of this NOI to the NSTIC implementation*:* Comments submitted on this Notice will serve as input for a Departmental report that will include a summary of responses to comments on this Notice, as well as the government's recommendations for the processes and structure necessary for the establishment and maintenance of a successful steering group.

The report will focus on the steering group in two phases: 1) the structure and functions of the steering group and 2) the initial establishment of the steering group. This report may include recommendations for addressing governance structures and processes for a variety of issues, including: leadership, representation of Identity Ecosystem participants; accountability measures; liability issues; accreditation and certification processes; cross-sector and cross-industry issues; the balance of self-interested and self-regulatory roles of steering group participants; adherence to the Guiding Principles; interaction and involvement with standards development organizations and other technical bodies; use, development, and maintenance of a trustmark scheme; the relationship of the steering group to the Federal government; and interactions with international governments and fora.

Request for Comment: This Notice of Inquiry seeks comment on the requirements of, and possible models for, 1) the structure and functions of the steering group and 2) the initial establishment of the steering group. Responses can include information detailing the effective and ineffective aspects of other governance models and how they apply to governance needs of the Identity Ecosystem, as well as feedback specific to requirements of the Strategy and governance solutions for those requirements. The questions below are intended to assist in framing the issues and should not be construed as a limitation on comments that parties may submit. The Department invites comment on the full range of issues that may be raised by this Notice. Comments that contain references to studies, research and other empirical data that are not widely published should be accompanied by copies of the referenced materials with the submitted comments, keeping in mind that all submissions will be part of public record.

The first section of this Notice addresses the steady-state structure of the steering group. The second section addresses the process of initiating a steering group that can evolve into that steady-state. The third and fourth sections address two fundamental aspects of governance both at initiation and steady-state: representation of stakeholders and international considerations.

1. Structure of the Steering Group

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 and economic landscape as the Identity Ecosystem Framework. The 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 and some of which are unregulated. The 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 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.

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?

Obviously the structure should align to the **scope** of the Steering Group as defined in the Strategy, which states:

> *Objective 1.4: Establish a steering group to administer the standards development and accreditation process for the Identity Ecosystem Framework.*

As you have rightly stated in the NOI, the Steering Group structure should be designed to operate in a manner most likely to produce outcomes compliant with the Guiding Principles as set forth in the Strategy, which are:

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

It logically follows that the Steering Group structure should be designed in a manner consistent with the **purpose** of the Strategy, which is to ensure the following vision is fulfilled:

> *Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.*

We therefore make the following recommendations for how to structure the Steering Group to effectively fulfill its mandate in a timely manner:

- **Scope: Responsibility and Authority**
  - Throughout the private sector engagement process that led to the development of the Strategy, a few key messages were consistently provided to the NSTIC authors from a multitude of sources that are helpful to recall as the NSTIC NPO translates certain high-level statements found in the Strategy into concrete operating policy for the Steering Group. We restate some of the most common private-sector comments on NSTIC in the context of our detailed recommendations below:
    - NSTIC is a document that defines a vision and strategy, informed by capturing input from a multitude of parties, but set forth by one (albeit quite influential) stakeholder in the Identity Ecosystem -- the US Federal Government.
    - As often stated by NSTIC spokespersons, there is cognitive dissonance in the title of the Strategy due to the fact that "cyberspace" is not "national", but quite significantly international. Therefore any ambition to have a significant effect on "Trusted Identities in Cyberspace" must also be significantly international in design.
    - To that end, we recommend that the NSTIC NPO refer to the

desired outcome of this effort as the "Global Identity Ecosystem" from this point forward.
        - We also encourage the NSTIC NPO to ensure the US Federal Government is fully represented and engaged as an equal stakeholder in the evolution of the Global Identity Ecosystem. This could be done by either having the NPO represent US Federal Government interests, or perhaps more effectively, by having each agency represent its own interests just as we would expect other national government agencies to do (see Representation below).
        - Both the private and public sector worldwide have been developing standards and accreditation processes for trusted digital assertions of identity for many years. These are investments to be leveraged by the Steering Group, not ignored or supplanted. We strongly encourage the NSTIC NPO to avoid the mistake of interpreting "administer the standards development and accreditation process" as an invitation to start over. What the global community of identity providers and relying parties needs from the Steering Group is adoption of existing solutions in the context of an overall vision.
    - With those key considerations in mind, we recommend the Steering Group be scoped specifically to "identify requirements" for the Global Identity Ecosystem, "identify candidate standards and accreditation programs" and to "perform a gap analysis" between the two. The Steering Group should also be chartered with the responsibility and authority to fill any gap they discover by first publishing those findings and providing a reasonable period for existing standards bodies and accreditation bodies to respond with proposals to fill that gap.
    - If the community does not respond with solutions to fill the gaps identified by the Steering Group in a timely manner, the US Federal Government could always turn to NIST to fill those gaps. This is the option of last resort however due to the highly likely scenario that any NIST standard or accreditation program would likely see very poor adoption by markets outside the US, and therefore poor adoption by international corporations.
    - At no point in its existence should the Steering Group be authorized to develop either technical standards or accreditation programs of its own design.
    - The Steering Group should have as its primary deliverable a set of "Recommendations" for the standards and accreditation programs identity providers and relying parties should adopt as a means of taking full advantage of the emerging Global Identity Ecosystem.
- **Participation and Governance:**
    - Given the diverse nature of the Global Identity Ecosystem stakeholders, we recommend a simple two-tier participation structure for the Steering Group:
        - A "Global Identity Ecosystem Steering Group Community" and
        - A "Global Identity Ecosystem Steering Group Council"
    - The Community body will be the superset of all those who choose to participate in deliberations conducted online or choose to travel

to in-person meetings of the Steering Group. No decision to endorse a standard or program will ever be made by the Steering Group without first providing a reasonable period of Community deliberation.

- This approach provides the Steering Group with flexibility to have certain administrative decisions made by the Council (for efficiency) and other substantive decisions made by the full Steering Group (the superset of all Council and Community participants).
- The Steering Group (Community and Council) shall always meet in public, with members of the Community invited to attend all meetings of the Council (though the Chair may need to limit discussion from time-to-time for the sake of making progress).
- The Steering Group Council will be comprised of Community members who have been elected to serve one-year terms. We suggest having ½ of the initial seats set for two-year terms so that the Council will only be subject to transition of no more than 50% of its members at any one time. Council members could be removed at any time by a vote of the Community.
- We recommend the NSTIC NPO not try to predetermine how many seats should be available on the Council or what the specific delineation of responsibility exists between the Council and the Community, but rather simply convene the Community and facilitate a set of bootstrapping decisions around the detailed scope and composition of the Council. We simply offer up the example of ANSI HITSP (Health Information Technology Standards Panel) as a potential model for how to successfully bootstrap an organization with many similarities to the Global Identity Ecosystem Steering Group (and we suggest the NSTIC NPO play the role ANSI did in HITSP).
- We recommend the Steering Group (both on the Council and Community) take a lesson from the IETF (Internet Engineering Task Force) and use the same notion of "rough consensus" as the primary means of driving progress forward. The Steering Group shall endeavor to make all decisions by rough consensus. Only when rough consensus cannot be reached in a timely manner shall any decision be put to a formal vote. Robert's Rules of Order should be observed.

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?

We have already mentioned ANSI HITSP as a model for how to initiate the formation of the Steering Group. But the best example of an ongoing organization with similar scale is Kantara Initiative. One of the key elements of its success, and we suggest will be a key element for any such organization to be successful, is having qualified professional support staff to manage communication, logistics, deliverables, IT support, etc.

Though we have made it clear that NSTIC NPO should participate in the Global Identity Ecosystem Steering Group as simply one of many stakeholders, it is not unreasonable for any one stakeholder to volunteer to bootstrap the operations of an effort like this for a fixed period of time.

We therefore recommend that NSTIC NPO volunteer to either fund an existing support organization (like Kantara Initiative) to perform these duties or volunteer its own staff and operating budget for a period of 24-36 months to ensure timely formation and deliberation of the Steering Group (this is essentially the role ANSI played in HITSP). Thereafter, if the Steering Group has demonstrated value as a facilitator of the Global Identity Ecosystem, the Steering Group will be able to sustaining its support staff through financial contributions from its stakeholder community.

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.

See 1.1 above.

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?

See 1.1 and 1.2 above.

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

The Global Identity Ecosystem has a clear set of stakeholders, if brought together in a manner consistent with our recommendations in 1.1, shall be able to address the needs of all stakeholders in a cohesive manner vs. trying to support different sectors differently. All sectors can participate in identifying the requirements and the Steering Group being mandated to close all gaps identified, shall be servicing all stakeholders equally.

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?

This question provides a teachable moment to reinforce our recommendation above regarding the proper international positioning of this effort. We recommend that future documents associated with this effort cease to use

the term "the government" when indicating US Federal Government and actually make it a point to explicitly position the US Federal Government as just one of many public sector stakeholders in this effort.

As to the question itself: Regulatory requirements will be provided by the regulated entities that engage at either the Council or Community level within the Steering Group. Therefore we believe the engagement model recommended herein shall efficiently address this concern.

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"[1] regulation from regulated participants in the Identity Ecosystem?

See 1.6 above.

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

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

Full stakeholder representation is the most critical success factor for the Steering Group. If NSTIC NPO can successfully position this effort as a truly Global Identity Ecosystem activity, with full support from (but not control by) the US Federal Government, then we suspect the Steering Group will have the level of broad stakeholder engagement it needs to be successful. If key sectors are not represented in the Steering Group, then this effort will likely fall short of the vision defined in the Strategy.

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?

See 1.1 and 1.2 above. The only difference between initiation stage and steady state should be NSTIC NPO's role in providing support staff and/or operating budget for the first 24-36 months.

2. Steering Group Initiation

In its role of supporting the private sector's leadership of the Identity Ecosystem, the government's aim is to accelerate establishment of a steering group that will uphold the Guiding Principles of the Strategy. The government thus seeks comment on the ways in which it can be a catalyst to the establishment of the steering group.

There are many means by which the steering group could be formed, and such structures generally fall into three broad categories:

a) A new organization, organically formed by interested stakeholders.
b) An existing stakeholder organization that establishes the steering group as part of its activities.
c) Use of government authorities, such as the Federal Advisory Committee Act (FACA),

to charge a new or existing advisory panel with formulating recommendations for the initial policy and technical framework for the Identity Ecosystem, allowing for a transition to a private sector body after establishing a sustainable Identity Ecosystem, or through the legislative process..

Questions:

All questions in this section are answered by our response in 1.1 and 1.2 above.

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?

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

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

2.4. 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?

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.

3. *Representation of Stakeholders in the Steering Group*

Representation of all stakeholders is a difficult but essential task when stakeholders are as numerous and diverse as those in the Identity Ecosystem. The breadth of stakeholder representation and the voice they have in policy formulation must be fair and transparent. The steering group must be accountable to all participants in the Identity Ecosystem, including individuals. An essential task for the steering group will be to provide organizations or individuals who may not be direct participants in the Identity Ecosystem, such as privacy and civil liberties advocacy groups, with a meaningful way to have an impact on policy formulation.

Given the diverse, multi-sector set of stakeholders in the Identity Ecosystem, representation in the steering group must be carefully balanced. Should the influence skew in any direction, stakeholders may quickly lose confidence in the ability of the steering group to fairly formulate solutions to the variety of issues that surround the creation and governance of the Identity Ecosystem.

Questions:

All questions in this section are answered by our response in 1.1 and 1.2 above.

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?

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

3.3. What does balanced representation mean and how can it be achieved? What steps

can be taken guard against disproportionate influence over policy formulation?

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?

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.

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

3.7. 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?

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 fora.

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.

Questions:

All questions in this section are primarily answered by our response in 1.1 and 1.2 above, with a few additional comments below.

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

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

We recommend that you reach out to your public sector peers within other governments and share your intentions to be a co-founding participant in the Global Identity Ecosystem through this Steering Group engagement model. Ask them to join you as a peer in forming the Steering Group to ensure the global marketplace meets their requirements.

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

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

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

Dated:

/ s /

Patrick Gallagher
Under Secretary of Commerce for Standards and Technology