1615 H Street, NW
Washington, DC 20062-2000
Tel: 202/463-3100
Fax: 202/463-3177
E-mail: abeauchesne@uschamber.com

U.S. Chamber of Commerce
www.uschamber.com

July 21, 2011

Ann Beauchesne
Vice President
National Security & Emergency Preparedness Department

Via e-mail: NSTICnoi@nist.gov

Mr. Jeremy Grant
Senior Executive Advisor for Identity Management
National Institute of Standards and Technology
100 Bureau Drive, Mailstop 8930
Gaithersburg, MD 20899

Dear Mr. Grant:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organizations of every size, sector, and region, thanks the Department of Commerce for collecting public comments on its Notice of Inquiry (NOI) titled "Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace (NSTIC)."[1] The NOI covers a wide range of promising topics for discussion and debate as well as a lengthy list of questions. The Chamber has not attempted to answer every question. Instead, we have focused mainly on the structure and representation of the governance body or "steering group."

Structure and Representation of the Steering Group

There are several governance structures that can perform some of the wide range of functions —technical, policy, legal, and otherwise — needed to formulate and administer the "Identity Ecosystem" that is envisioned by the NSTIC. The Chamber offers two models for the National Institute for Standards and Technology (NIST) to consider as it goes about establishing a new NSTIC steering group.

[1] www.nist.gov/nstic/nstic-frn-noi.pdf; docket no. 110524296-1289-02

Smart Grid: SGIP Organization

First, on June 9, 2011, George Arnold, NIST's National Coordinator for Smart Grid Interoperability, presented on the Smart Grid Interoperability Panel (SGIP) as a possible governance model for the Identity Ecosystem. He highlighted the following points, which could contribute positively to the thinking behind structure and representation of the steering group:

- The SGIP panel functions as a *public-private partnership*, which will be critical to the success of any governing body.
- It is open and transparent, consensus-based, and involves international participants.
- It coordinates standards developed by multiple standards-development organizations (e.g., International Organization for Standardization or ISO).
- The number and breadth of stakeholders is substantial.
- The panel is currently federally-funded; it may transition to a privately administered organization.

Page 7 of Mr. Arnold's presentation[2] provides a helpful, visual depiction of the SGIP organization. It features an SGIP governing board; and the board is complemented by a larger plenary group that includes additional stakeholder representation, such as a working group devoted to cybersecurity and various standing committees. Importantly, the plenary operates according to the principle of "one organization, one vote," which would be a reasonable approach for NSTIC steering group voting rights.

Critical Infrastructure Protection: NIPP Framework and CIPAC

Second, the National Infrastructure Protection Plan (NIPP) provides the overarching framework for public-private partnerships between government and the private sector for protecting our nation's critical infrastructure. The Critical Infrastructure Partnership Advisory Council (CIPAC) provides the operational mechanism for carrying out the NIPP framework. The CIPAC provides the structure for owner/operator members of Sector Coordinating Councils (SCC) and members of Government Coordinating Councils (GCC) to engage in intra-government and public-private cooperation, information sharing, and engagement across the entire range of critical infrastructure protection activities.

Ideally, the successful execution of the sector partnership structure requires an environment in which members of the SCCs and GCCs can interact freely and share sensitive information and advice about threats, vulnerabilities, protective measures, and lessons learned. CIPAC, which has been exempted from the requirements of the Federal Advisory Committee Act (FACA), is the mechanism to allow meaningful dialogue on key critical infrastructure protection issues and agreement on mutual action between government and owner/operator entities. Individuals who are registered to lobby should be able to sit on the steering group.[3]

[2] www.nist.gov/nstic/presentations/arnold.pdf

[3] www.dhs.gov/files/programs/editorial_0827.shtm

The NSTIC calls for creating a public-private steering group that will administer the process for policy and technical standards development for the Identity Ecosystem, while facilitating input from interested stakeholders. The steering group will help drive implementation of the Identity Ecosystem and track progress toward meeting short- and long-term benchmarks. Such a group, leveraging the CIPAC model, could meet 3-4 times per year to provide high-level visibility and coordination, foster accountability and adjudicate disputes, and improve decision-making.

Private sector representatives on the NSTIC steering group should include key CIPAC organizations, such as the information technology (IT), communications, financial, energy, and transportation SCCs as well as the Cross Sector Cyber Security Working Group. Further, relevant industry associations should have appropriate representation on the steering group. The private sector will play a very important role in leading the steering group. Among the successful aspects of an SCC that NIST can draw lessons from include:

- Its charter or bylaws are developed through an open and consensus-driven process.
- It features a small group of leaders or officers who are accountable to the plenary (they are elected by the plenary and can be recalled or removed from office).
- The board or executive committee is allotted a specific numbers of seats to accommodate specific sub-sector representatives and who are similarly accountable (i.e., elected).
- The SCC plenary is open to all who are members of the sector, according to consensus-driven guidelines written by plenary participants.
- Membership in the plenary is encouraged through free membership. Government partners cover relatively minor, administrative-support costs; some private-sector entities contribute in-kind resources (e.g., space for meetings).
- Working groups are formed, as needed, and overseen by the executive committee and officers, who report quarterly to the plenary. The working groups are led by the private sector but encourage government participation for joint efforts (e.g., roadmaps to secure control systems, the IT Sector Baseline Risk Assessment).

The Chamber believes that any new steering group should act primarily as a “traffic cop,” helping to guide private sector entities wrestle with standards adoption and technical issues as they design and implement the Identity Ecosystem rather than acting as a vigorous rulemaking authority.

In terms of administering the processes for policy and standards adoption, the Chamber believes that NIST should take the lead in promoting the adoption of international cybersecurity standards and best practices developed by industry-led and/or public-private standards-development bodies.[4] Whatever form the governing council takes, NIST needs to ensure coordination with international stakeholders like the ISO. Non-U.S. participation will help ensure that the Identity Ecosystem that emerges is usable by multinational companies and other organizations.

[4] See the Chamber’s March 7, 20011, comments to the Commerce Department regarding the government’s role in the standards-setting process.

The Chamber also believes that the steering group should be small enough to be effective but large enough to be inclusive. There is no magic number, but NIST could consider including 10-20 members on the steering group's governing board. The plenary group could include twice this number of members.

It is unclear to what extent NIST envisions government agencies and departments (e.g., Commerce and Homeland Security) being represented on the steering group. The Chamber believes participation by government officials is vital but that they should hold a limited number (e.g., approximately 25%) of seats on the steering group. In sum, among the points the Chamber seeks to stress are:

- The steering group, which needs to be as inclusive as possible yet remain effective, must be initiated as a public-private partnership; potential models include the SGIP and the CIPAC. NIST should blend the strengths of both groups together.

- The steering group should act primarily as a "traffic cop," helping private sector entities navigate issues related to standards adoption or legal issues rather than acting primarily as a rulemaking authority.

- The steering group should view standards adoption from a global perspective. NIST should ensure coordination with international stakeholders, which the SGIP seems to emphasize. Non-U.S. participation will help ensure that the Identity Ecosystem will be usable by multinational companies and organizations.

- The steering group should be exempted from the requirements of the FACA, a key feature of the NIPP/CIPAC model, to facilitate meaningful dialogue among participants, including registered lobbyists.

- Participation should perhaps be free to encourage inclusiveness. Businesses could offer in-kind support (e.g., meeting space); government should shoulder basic administrative expenses.

The Chamber welcomes the Department of Commerce's review of models for a governance body to administer the processes for policy and standards adoption for the Identity Ecosystem framework. The Chamber was extremely honored to host the White House for the unveiling of the NSTIC on April 15. We look forward to continuing to work with the Department and NIST as the private sector and its government partners implement the NSTIC.

Sincerely,

Ann Beauchesne

Ann Beauchesne