July 22, 2011

Submitted via email to NSTICnoi@nist.gov
Annie Sokol
National Institute of Standards and Technology
100 Bureau Drive, Mailstop 8930
Gaithersburg, MD 20899

RE: FSSCC Comments on Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace (Docket No. 110524296-1289-02)

The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security ("FSSCC") appreciates the opportunity to comment on the Notice of Inquiry on Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace (NSTIC). The NOI seeks comments on the formation and structure, functions and processes of the governance body referred to in the NSTIC as "the Steering Group." The Steering Group would administer the process for policy and standards development for the "Identity Ecosystem Framework" in accordance with the Strategy's Guiding Principles that identity solutions must be: privacy-enhancing and voluntary, secure and resilient, interoperable, cost-effective, and easy to use.

The following provides background information on the FSSCC and our comments on the structure, representation, and role of the Steering Group.

Background on FSSCC

The FSSCC was established in 2002 in response to the September 11, 2001 attacks and at the request of the U.S. Treasury Department in harmony with several Presidential Directives requiring sector-specific Federal departments and agencies to identify, prioritize, and protect United States critical infrastructure and key resources and to establish partnerships with the private sector. The FSSCC has 52 member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government sponsored enterprises, investment banks, merchants, retail banks, and electronic payment firms.

The FSSCC has had a long-standing interest in improving identity assurance and has been supportive of the development of the NSTIC. In recent years, the FSSCC has focused considerable attention on improving identity assurance. Our collaboration resulted in a groundbreaking Memorandum of Understanding (MOU), which was signed on December 6, 2010 by the FSSCC, DHS, and the National Institute of Standards and Technology (NIST) with active support by the White House Cybersecurity Advisor and head of the Office of Science and Technology Policy. The MOU lays the foundation for developing an identity assurance test bed that will focus on improving the accuracy and timeliness of identity proofing and reducing identity impersonation. The collaborative initiative includes the concept of a "financial services verification identity credential system" to enable direct verification of identity credentials with the authenticating authorities. Presently, the FSSCC is working with DHS and NIST on a Cooperative Research and Development Agreement (CRADA) on identity proofing. Also envisioned in the MOU is an effort to define and test the concept of establishing a secure domain within the larger Internet, where critical industries and government can more securely exchange sensitive information and complete high risk transactions.

NSTIC Steering Group Comments and Recommendations

Structure and Representation

Given the broad scope of the NSTIC and the role that the Steering Group would play in administering policy and standards development, there are two options for the legal structure of the group. The first would be a non-profit public benefit corporation and the second would be a federal advisory committee that would fall under the Federal Advisory Committee Act (FACA). While both models can succeed, the FSSCC believes the non-profit public benefit corporation model would provide greater flexibility to administer the process for policy and standards development so long as the non-profit public benefit corporation has clearly defined articles of incorporation and bylaws. An example of an existing non-profit public benefit corporation that is similar in the number and diversity of global interests is the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN has a board of directors whose composition rotates and is voted on by the members. It also has several working groups and committees, an ombudsman, a president and CEO and a full time staff.

The FSSCC recommends that that the Steering Group be representative, manageable, and accountable. In order for the Steering Group to be manageable and to attract talented professionals, the FSSCC recommends that the Steering Group consist of no more than 15 members. It should include representatives from critical infrastructure sectors (e.g., Communications, Finance, Transportation), academia, and standards body (e.g., ANSI). These representatives should have a variety of experts in legal/regulatory, behavior sciences, privacy and security and have knowledge of international issues. In addition, there should be public sector participation at both the Federal and state levels.

The FSSCC believes that financial services sector should be represented on the Steering Group because the sector needs high levels of assurance for secure transaction and

privacy protection. In addition, the sector is experienced in deploying complex systems that balance security requirements, privacy protections and comply with regulatory requirements. Examples of these include: "Know Your Customer", data security, privacy and vendor management regulations. From a security viewpoint, the financial services sector is a prime target for cyber criminals, experiencing daily attacks. Finally, the financial services sector is actively involved in the implementation of the NSTIC through a pilot on identity proofing.

While the FSSCC believes that it would be challenging to recruit top talent for this Steering Group if it is too large, it could be augmented by a number of working committees that would tap the needed expertise (e.g., legal, technical, business models, regulatory, international) to address various issues and tasks in parallel, while still giving all stakeholders an opportunity to weigh in on all issues and decisions.

Additionally, the FSSCC recommends that the deliberations of the Steering Group be open and transparent, with opportunities for public input. Hence, the governance documents (e.g., charter, by-laws) should include a defined process to support the goal of an open and transparent process.

Because of this current lack of definition and operational experience, and uncertainty regarding market place acceptance and what ultimately the identity ecosystem will look like, the FSSCC recommends that the policies, guidance and standards issued by the NSTIC Steering Group not be overly prescriptive and favor broad guidelines (e.g., identifying the need for a framework/solution to address security and privacy concerns and processes resolving disputes). Hence, the guidelines and standards should be sufficiently flexible to allow for a diversity of approaches; letting the marketplace pick the winners and losers. It should recognize that different groups have different needs that can lead to many different types of frameworks needing to co-exist and interoperate. They should allow a wide range of business models, technical approaches and process flows, requiring only the minimal standards necessary to permit interoperability amongst approaches.

Further, the identity ecosystem will need to change and evolve over time in response to changing requirements, application functionality and technology, and the guidelines and standards will need to accommodate this evolution. The NSTIC Steering Group should allow for a "learning through doing approach" given that change is likely and there will be a need to respond to changes in the threat landscape, technology and consumer behavior and attitudes. This may include loosening up existing standards to allow greater decoupling of identity proofing assurance levels from authentication assurance levels, and greater granularity of assurance levels. Above all, the governance model must be structured to empower the private sector.

Role in Establishing Pilots

The Steering Group could initially be set-up to oversee government and industry-initiated identity ecosystem pilots. In this way it could be seeded with participants of these pilots and other interested parties. As pilots are deployed, the Steering Group could transition from overseeing pilots to overseeing operational deployment. The Government should be

prepared to pay for start-up and administration costs, for at least the pilot period. The private sector will need to pick-up their own costs of travel and resources, with grants available to ensure participation of small organizations with limited funding.

Thank you for the opportunity to comment. Please let me know if you have any questions or if the FSSCC can provide additional information.

Jane D. Carlin

Chairperson of the Financial Services Sector Coordinating Council
Managing Director of Morgan Stanley