THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Response to the National Strategy for Secure Online Transactions

May 6, 2010

May 6, 2010
Enclosure 1: NSTAC Comments on the Partial Draft version 0.1,
***National Strategy for Secure Online Transactions* (NSSOT), dated April 23, 2010**

1.0 INTRODUCTION AND SUMMARY

Identity has long been a recognized concern of the networked business community. The President's National Security Telecommunications Advisory Committee (NSTAC) recommendations in many past reports, especially since 2005[1], though focused in different areas, touched on aspects of identity issues, and included specific recommendations[2]. The growing criticality of identity issues in network operations culminated in the May 2009 *NSTAC Report to the President on Identity Management Strategy* and recommendations therein specifically focused on identity issues and strategy.[3] We are delighted to find that numerous aspects of that report have been embraced in the *National Strategy for Secure Online Transactions* (NSSOT) draft. The NSSOT is a timely initiative and important as a reasonable next step toward comprehensive and collaborative government-industry solutions needed in this area.

The NSTAC is encouraged that in this draft, Government has taken a top-down approach to a key aspect of identifiability and the application of personally identifiable information (PII) to specific contexts. In so doing, the value of successful outcomes is made largely self-evident, in that specific, important identity-sensitive transactions may be conducted as desired and necessary. By placing emphasis on the whole range of organizational and individual end users, these may see personal value in supporting needed steps, including those of a highly-technical nature, to secure online transactions. These users, taken together, will define the specific functionality needed, and thereby more precisely and efficiently guide the efforts of organizations and programs designed to deliver those capabilities. In this way, not only technology processes in Government and industry, but also domestic and international policy considerations may be highlighted for attention.

Comments on specific sections of the April 23, 2010, draft version 0.1 NSSOT follow.

2.0 VISION AND VALUE PROPOSITION

The NSTAC believes that this section would benefit by taking a broader approach to the profound impact that would result from the successful achievement of the goals of the NSSOT in public and private life. Benefits here are characterized as being applicable to "individuals, the private sector and government," and in some cases, the listed benefits are indeed unique to those groups. However, the higher-order understanding remains unstated, namely that the end effect of

[1] *NSTAC Next-Generation Network Near-Term Recommendations Working Group Report*, March 2005, Recommendation 4.
[2] These include, *inter alia*, *NSTAC Next-Generation Network Near-Term Recommendations Working Group Report*, March 2005; *NSTAC Next Generation Networks Task Force Report*, March 2006; *NGN Implementation Annex Working Group Letter to the President*, November 2008; *NSTAC Response to the Sixty-Day Cyber Study Group*, March 12, 2009; and *NSTAC Cybersecurity Collaboration Report*, May 2009.
[3] *NSTAC Report to the President on Identity Management Strategy*, May 2009.

securing online transactions would be enhanced economic security, and that in turn is tantamount to national security, with beneficial effect across the board for all—individuals, organizations and Government.

It is clear that in an undertaking of such enormous scope, complexity and importance to all sectors of society, a rigorous government-civil partnership will be necessary to ensure success. The NSTAC notes that the draft calls for such a partnership. We look forward to working with the Administration, helping to design, implement and operate collaborative approaches that achieve needed functionality while preserving personal privacy, liberty, and freedom of action for citizens and businesses.

In that regard, one key aspect of the value proposition needs to be underlined, namely the degree to which the NSSOT, if and when successfully implemented, will serve as an enabler across the board. The enablement of personal choice, of confident online engagement, of the extension of new services, functions and features by online service providers and Government—all of these are embedded virtues within the NSSOT, and should be clearly stated as such.

A second key need within the value proposition is the assertion of transparency, even auditability, of sensitive processes to which individuals and organizations are a party. This would be a universal good within the system, equally applicable to consumers, businesses, and governments at every level.

3.0 GOALS AND OBJECTIVES

3.1 Enhance the Security of Online Transactions Through Development of a Common, Comprehensive Trust Framework.

The governance framework called for here is certainly necessary. It is important to specify the precise roles, missions, responsibilities, and authorities of Government, industry service providers, and end user organizations and individuals, within such a structure. All of these will have roles, and must be empowered in order for something as broadly-impacting as the NSSOT to succeed.[4]

Within Government, we continue to believe that this process will be enhanced by the establishment of a single, authoritative, and comprehensive organizational focal point for identity issues within the Executive Office of the President.[5] This will facilitate coordination with the many and various engaged stakeholders external to Government.

Governance will be influenced by the expectation that in future as at present, there will not be a single identity trust framework for online transactions, but multiple ones. Governance must therefore take the form of guidelines and "boundary conditions," rather than an overly-prescriptive set of rules that will be unable to keep pace with technical and market development. In this way, all stakeholders, from relying parties and end users to identity-service providers, will see both opportunity and benefit from the NSSOT. Government can be very

[4] *Ibid*, Recommendation 3.
[5] *Ibid*, Recommendation 2.

helpful in this process through active promotion of the development and adoption of voluntary standards, a point raised in Goal #5 as it relates to international engagement. The NSTAC has long supported rigorous standards development, not only as an enabler of security functions, but to encourage investment based on confidence in stable technology policy.[6]

3.2 Build and Implement Interoperable Infrastructure Aligned with the Common Trust Framework.

As noted, the respective roles and missions of Government and industry must be clearly established in the design of trust frameworks. As that design moves toward implementation across the national web-based domain, it is clear that the preponderance of work here will actually be conducted outside Government. This serves to underline the criticality of preserving opportunity for innovation, initiative, and entrepreneurship in the process. The NSTAC stands ready to work closely with Government in such a collaborative process, as recommended in several reports in recent years.[7]

3.3 Enhance Confidence and Participation in Online Services

The point raised earlier regarding "enablement" could be repeated here. Nothing more clearly implicates the need for a genuine, across-the-board partnership than this issue, wherein confidence will be engendered by the combined efforts of all national stakeholders.

Effective, sustained, and multi-level strategic communications and public outreach will be critical in this area. Such efforts will be particularly useful and necessary to ameliorate privacy and civil liberty concerns through education and the portrayal of personal value.[8]

3.4 Increase Security Knowledge and Awareness Among Participants in Online Transactions

As trusted partners and collaborators in a shared purpose, Government and industry may and must learn from each other. This understanding has been at the core of NSTAC efforts in recent years, including the current pilot program to test the draft concept of operations for the private sector component of the NSTAC recommended Joint Coordinating Center.[9]

3.5 Coordinate and Lead National and International Efforts to Drive Innovation, Interoperability, and Trust

As mentioned in section 3.1 above, the NSTAC continues to believe that this process will be enhanced by the establishment of a single, authoritative, and comprehensive organizational focal point for identity issues within the Executive Office of the President.[10] This will facilitate coordination with the many and various engaged stakeholders external to Government. To this

[6] *NSTAC Next-Generation Network Near-Term Recommendations Working Group Report*, March 2005, Recommendation 7.
[7] *NGN Implementation Annex Working Group Letter to the President*, November 2008, Recommendation 1; *NSTAC Next Generation Networks Task Force Report*, March 2006, Recommendation 1; *inter alia*
[8] *NSTAC Report to the President on Identity Management Strategy*, May 2009, Recommendation 3.
[9] *NSTAC Cybersecurity Collaboration Report*, May 2009, Recommendation 1.
[10] *NSTAC Report to the President on Identity Management Strategy*, May 2009, Recommendation 2.

end, the Federal Government should increase its support to, and participation in, international standards creation and development related to identity issues.[11]

The beneficial role of standards development here cannot be overstated. The NSTAC urges focused and sustained engagement in this area to advance NSSOT objectives in several areas.[12]

As a related matter, research and development will indeed be needed, and focused Governmental investment will be very beneficial.[13]

The NSTAC strongly endorses recognition of the complex and interrelated relationship between the domains of cybersecurity and online transaction identity. This fundamental characteristic of the network universe has been recognized by NSTAC[14] and related organizational studies in recent years. It demands a careful and integrated approach, in order to achieve security while preserving privacy and civil liberty.

4.0 APPENDIX A – GLOSSARY

In the May 2009 *NSTAC Report to the President on Identity Management Strategy*, NSTAC chose to adopt the glossary then being used by the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T)[15] in its ongoing standards and policy efforts in the same field. This approach was also taken by the National Science and Technology Committee's Subcommittee on Identity Management in its interagency Task Force on Identity Management.[16] Accordingly, NSTAC recommends that in the interest of convergence on more broadly-accepted and authoritative definitions in identity-related areas, the government should also adopt the ITU-T glossary for the NSSOT and contribute to its evolution.

[11] *Ibid*, Recommendation 3.
[12] *NSTAC Next-Generation Network Near-Term Recommendations Working Group Report*, March 2005, Recommendation 7.
[13] *NGN Implementation Annex Working Group Letter to the President*, November 2008, Recommendation 1.
[14] *NSTAC Report to the President on Identity Management Strategy*, May 2009.
[15] *Ibid*, Appendix C – Definitions.
[16] National Science and Technology Council: Subcommittee on Biometrics and Identity Management, *Identity Management Task Force Report 2008*, July 2008, http://www.biometrics.gov/Documents/IdMReport_22SEP08_Final.pdf