THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Response to the National Strategy for Secure Online Transactions
Partial Draft version 0.2

June 2010

1.0 INTRODUCTION AND SCOPE

The draft *National Strategy for Secure Online Transactions* (NSSOT) acknowledges that "identity" is much broader, in both policy and technology, than is addressed within the document's scope.[1] Nevertheless, the National Security Telecommunications Advisory Committee (NSTAC) believes that structures and strategies created to address NSSOT must be designed to be extensible to the needs of all relevant business and social interests ultimately involved in the larger identity issue. In this way, structures and strategies developed in the formative stages of the NSSOT can anticipate and eventually support expanded requirements as the Executive Office of the President (EOP) begins to address other topics within identity management.

NSTAC understands that the NSSOT's scope is intended to include all electronic "transactions" as defined in the document, including those between Federal Government agencies and any individual or organization with which they may interact, as well as between business and consumers where Government is not a direct participant in the transaction. This solution enables the NSSOT to develop approaches specific to online identity as it relates to transactions, while making clear that "identity in America" includes much more than the NSSOT encompasses. At the same time, this approach helps identify the broad range of communities and organizations that will participate and contribute in this area, both inside Government and across society. There is also a need to recognize and engage in related international activities in order for this endeavor to be successful. Developing this understanding at the outset will allow stakeholders to work together to advance the government/business/social agenda in identity and identifiability—beginning with the NSSOT, but continuing thereafter as needed.

The NSTAC believes that this approach adds value to the draft NSSOT. Specifically:

- The NSSOT focuses on a small segment of the Federal Government compared to the total realm of identity issues, programs, and processes across Government, throughout society, and internationally. The draft only briefly mentions the Department of Defense; Department of Justice; the Intelligence Community or citizen-facing organizations such as the Department of Health and Human Services and the Department of Veterans Affairs. In addition, the draft does not make any mention of topically-specific Federal Government organizations that interact with industry on regulatory and policy oversight issues, including the Department of Treasury, the Federal Communications Commission (FCC), or Federal Aviation Administration. Outside of Government, identity sensitive technologies and processes are being developed and fielded at an accelerating rate in every segment of industry and society. Health care and financial services sectors both show strong need in these areas. International standards bodies are actively developing relevant standards. Many of the public and private activities cited here, both domestic and international, have impact on identifiability in ways that the NSSOT does not address within its defined scope as drafted.
- The draft refers to an "identity ecosystem," which the NSTAC considers an important and useful conceptual construct. However, rather than being narrowly drawn within the NSSOT's

[1] *National Strategy for Secure Online Transactions (NSSOT),* Partial Draft Version 0.2, pg 4 line 94.

defined scope, that concept should extend to the total domain of identifiability, including those issues and applications that have no online component whatsoever. The NSTAC continues to urge broad treatment of identity in Government and commerce, in both physical and cyberspace dimensions, where the magnitude of opportunities, pitfalls, and consequences of misdirection and inaction are more apparent.[2] The NSTAC believes this expanded view is a more accurate description of the identity ecosystem. The NSTAC further believes this approach will encourage greater interaction between Government and the private sector as they work to achieve common goals and address national needs, especially in areas such as international engagement and research.[3]

2.0 GOVERNANCE

The NSSOT's limited scope directly impacts the proposed governance models and processes envisioned in the draft strategy. The NSTAC affirms its findings in the 2009 *NSTAC Report to the President on Identity Management Strategy* regarding the proper and needed focus of identity policy within and across the Federal Government. Specifically, the NSTAC believes that, due to the vastness and universal applicability of identity, the President must expressly retain policy, budgetary, and interagency-coordination authority.[4]

Specifically, the NSTAC believes that three distinct domains require oversight and influence: policy oversight, independent advice, and daily governance. These domains are complementary processes, with none being able to substitute for any other.

Policy Oversight: As noted, the NSTAC believes that EOP should retain policy oversight. Reasons include:

- Topical Linkage: Numerous recent studies have noted that an as-yet undefined intersection exists between identity and cybersecurity in policy, technology, and programs.[5] Specifically, identity issues at the core of the NSSOT are topically linked to the *Comprehensive National Cybersecurity Initiative* (CNCI). In that area, several key Federal departments and agencies are responsible for executing the CNCI, while the EOP maintains policy control. If this organization model is applied to the NSSOT, it could influence progress in understanding, treating, and deconflicting overlapping cyber/identity equities and issues. Shifting NSSOT management to the departmental level could potentially harm aspects of economic security, national security, emergency preparedness and homeland security.

[2] *NSTAC Report to the President on Identity Management Strategy*, May 2009, page 20. http://www.ncs.gov/nstac/reports/2009/NSTAC%20IDTF%20Report.pdf

[3] For example, as supported in National Science and Technology Committee's *Identity Management Task Force Report 2008*, http://www.biometrics.gov/Documents/IdMReport_22SEP08_Final.pdf; *NSTAC Report to the President on Identity Management Strategy*, May 2009, http://www.ncs.gov/nstac/reports/2009/NSTAC%20IDTF%20Report.pdf; *Cybersecurity Policy Review*, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[4] *Ibid*, Recommendation 3, page 24.

[5] National Science and Technology Committee's *Identity Management Task Force Report 2008*, http://www.biometrics.gov/Documents/IdMReport_22SEP08_Final.pdf; *NSTAC Report to the President on Identity Management Strategy*, May 2009, http://www.ncs.gov/nstac/reports/2009/NSTAC%20IDTF%20Report.pdf; *Cybersecurity Policy Review*, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

- Interagency Implications: Numerous Federal organizations have extensive, mission-critical interests in identity policy and technology. The EOP is uniquely positioned to effectively manage those cross-organizational relationships with the required authority. Many identity-sensitive programs and processes exist across government that are not currently available for online access or use. Although these programs do not presently fall within the NSSOT's scope, many may become online-enabled in time. Doing so would possibly shift NSSOT's focus, both within the Federal Government and as regards the Federal-civil interface. Such a shift may have consequences for Government organizational roles, missions and responsibilities. By retaining the policy, research and strategic lead, the EOP can anticipate and/or respond to any such trends as they become evident.
- Funding: The NSSOT emphasizes expanding research efforts, pilot technology, and grants to further examine identity issues, which, while laudable, draws attention to the need to identify and secure funding sources for such efforts. At present, these proposed efforts have programmatic links to several Federal organizations and appropriations authorities and, in some cases, non-governmental funding sources. EOP-level oversight may be required to manage these processes to ensure fairness among all parties and responsiveness to the highest-priority needs. Again, the EOP can assure priority attention to economic security, national security, emergency preparedness and homeland security.

Independent Advice: The NSSOT outlines an advisory process to obtain the advice and insights of leading thinkers and practitioners in relevant fields.[6] The NSTAC expressly endorses establishing and organizing this advisory process within the *Federal Advisory Committee Act* (FACA) framework, allowing proper transparency and public access inherent in FACA.

Operational Governance : A governance process such as that described in the draft is also essential to achieving the NSSOT's long-term and broadly-based objectives.[7] Separating this process of detailed daily management from policy oversight is appropriate and compatible with the NSTAC's basic recommendation to retain policy authority in the EOP.

The governance process must provide and perform several important functions as a minimum:

- Above all, institutionalized and broadly-based Government-private sector collaboration must occur on a deep and continuous basis. This collaboration requires full-time participation by multiple organizations across Government, as well as numerous individuals and organizations outside Government. Given the NSSOT's scope and impact, participants should represent key industries and citizen advocacy groups, and must provide sufficient transparency and reasonable access to private citizens. The degree of collaboration required cannot be overstated; failure to achieve this degree of inclusivity would seriously compromise the NSSOT's ability to be publicly accepted and effective.
- Organizers must also identify and retain funding sources to support long-term research, project planning, and task management for the diverse roles set forth in the draft.

[6] *NSSOT* Partial Draft Version 0.2, page 30, line 1092.
[7] *Ibid,* page 29, line 1065.

- Those individuals and organizations must clearly delineate NSSOT governance roles, missions, and responsibilities at the outset; this transparency will position the NSSOT's participating organizations for success and enhance public acceptance.
- Specific authorities provided to this initiative, including for Government-civil collaboration, may need to be established by Executive Order or in law, as appropriate, especially as regards any role in setting or enforcement of procedures or practices. Authorities must be sufficient to:

  −Elevate the issue to its intended national scope;

  −Provide specific and roles and responsibilities;

  −Support balancing national equities;

  −Facilitate consistent resource support; and

  −Provide for public transparency and accountability.

The governance functions must be implemented in a purpose-built organization. The organization may be modeled on a National Program Office structure, as the strategy proposes and as the NSTAC first recommended in 2009 [8]; or it might be structured on some other suitable organizational model. The NSTAC has made the case for establishing a universal conceptual approach to identity and identifiability. Therefore, NSTAC recommends that the chosen governance organization be similarly scoped, chartered, authorized, and resourced. Further, the establishing authorities must ensure the needed broad basis of long term, national support is available on an institutionalized basis. In this way, the governance structure needed to support the implications of expanding Governmental engagement in identity issues broadly will be accounted for at the outset, permitting smoother future development.

It is important to note that whatever organizational model is embraced, the NSSOT's total scope must extend beyond research and pilot technology projects to eventually include operational models and programs. These programs may be large in scale with significant economic and/or social impact, either initially or eventually. Any efforts on such a scale will necessarily require broad engagement of leading organizations in industry and elsewhere. This understanding reinforces the conviction of the NSTAC that for NSSOT to be approached and to succeed as a national undertaking requires careful consideration to management and inclusivity, from the initial planning stages forward.

3.0 RECOMMENDATIONS

Based on the authorities and responsibilities established by Executive Order 12472, Assignment *of National Security and Emergency Preparedness Telecommunications Functions*, the NSTAC recommends that the President:

- Recast the identity ecosystem concept by broadening its scope to include all persons, objects, devices, and data (including metadata), within which secure online transactions occur.[9]

[8] *NSTAC Report to the President on Identity Management Strategy*, May 2009.

[9] The NSTAC recognizes that the NSSOT's scope is limited and is intended to be a subset of the much-larger identity ecosystem concept.

- Expressly note that the NSSOT is a subset of the much-larger concept of identity and identification; describe and define the NSSOT's limited scope.
- Within the Federal Government, expressly establish the EOP as the policy lead for identifiability issues in general and the identity ecosystem specifically. As part of this policy lead position, the EOP also would be responsible for policy oversight and compliance.
- Identify an organizational model upon which to establish the NSSOT governance structure as described in Section 2.0. Potential models include:
  - Establishing a National Program Office;
  - Assigning the NSSOT governance structure to a subordinate body within the National Academy of Sciences;
  - Establishing an independent commission to carry out specific functions; or
  - Creating an appropriate new/hybrid approach.
- When crafting, executing and implementing the NSSOT, the EOP must be mindful of pending cybersecurity activities, including the FCC's proceeding on the Cyber Security Certification Program, PS Docket No. 10-93, Notice of Inquiry (NOI; FCC 10-63), released April 21, 2010. The perception of competing or uncoordinated Government efforts in identity can inhibit necessary collaboration and progress.
- Focus on a few key vertical areas (e.g. health care, financial services) for development of pilot technology, procedures and processes, that can eventually have wider application, in accordance with previous NSTAC recommendations.[10] This approach:
  - Permits economical initial expenditures to demonstrate proof of concept and program value;
  - Accelerates the pace at which modifications can be made to service infrastructure and business rules, as needed to change underlying processes;
  - Facilitates direct comparison between the "target sector" and others using legacy approaches, thereby supporting measurable cost/benefit analyses; and
  - Permits and encourages engagement with industry, states, congressional and private sector stakeholders, resulting in more rapid initial progress plus improved efficiency.
- The NSTAC continues to strongly endorse the national character of the NSSOT, even while recognizing the need to address the topic on a global scale, seeking to advance a national agenda where possible. At the same time, however, it recognizes that basic legal authorities through which Government can impose behavioral norms on industry and society are limited. Some provisions of the draft that refer to the anticipated Government-industry relationships provoke concern related to practicality, inhibition of commercial initiative and opportunity, and feasibility under the law. While the NSTAC expects the EOP would resolve many of these concerns in the course of implementing the recommendations above, the NSTAC believes the Government should not seek to control the huge process of online transaction to

[10] *NSTAC Report to the President on Identity Management Strategy,* May 2009.

the extent of developing and/or selecting brands, along lines suggested in NSSOT actions A7 and A8.[11] Instead, the NSTAC recommends that the Government focus on positive incentives, such as liability safe-harbor, as outlined in action A4 and elsewhere, and leverage existing and emergent trust brands conformant to standards.[12] Industry currently offers several such trust mark brands and, if necessary, will compete for any business resulting from policies such as those proposed in the NSSOT. This competition will stimulate optimal quality, pricing, and creativity to meet changing needs.

- Related to the above and in general, the EOP should continue to develop the role of commercial providers of identity and trust applications and services to create incentives for these parties to cooperate and collaborate. Linking relevant standards-setting processes is one area that would result in mutual benefit from expanded international engagement as a "national team". This is consistent with points raised in the draft, including action A32.[13]
- The NSTAC strongly endorses the current draft's explicit commitment to consumer privacy protections, but urges careful application of Fair Information Practice Principles (FIPPs) as part of the NSSOT. FIPPs are aligned, but do not exactly correspond, to identity verification and security requirements. Many identity verification systems in use today depend on robust information sharing, including those relied by on Fortune 100 telecommunications companies, financial institutions, and other credit issuers. Unqualified restrictions on data sharing, data retention, and data aggregation would severely impair these and future technologies. The NSTAC also notes that identification of an individual is an important predicate to many key privacy protections such as preventing identity theft, opting-out of unsolicited communications, and granting consumers access to records. Therefore, since FIPPs touch on privacy issues much beyond the scope of secure online transactions, NSTAC recommends that while FIPPs be addressed within the NSSOT where applicable, such treatment should not extend to legislative mandates.
- Transparency, public access, and accountability will be essential to build public and private trust and confidence in the NSSOT, as suggested in action A30.[14] The NSTAC therefore recommends that the EOP select the *Federal Advisory Committee Act* model over that of the Critical Infrastructure Partnership Advisory Committee, compared in action A29, as the basis for the advisory group proposed in that action.[15]

The NSTAC also recommends two technical revisions:

- In action A37, the NSTAC recommends the EOP delete "since the national strategy advocates a user that chooses to carry a single, strongly-identified credential".[16] This clause is inconsistent with the rest of the document, which discusses a vision of multiple credential and trust frameworks for various applications, emphasizing user choice as a primary determinant. Also, a one-credential approach is considered to be neither technically feasible, nor programmatically practical.

[11] *NSSOT* Partial Draft Version 0.2, pg 23, lines 792 and 809.
[12] *Ibid* pg 22, line 762.
[13] *Ibid*, pg 30, line 1108.
[14] *Ibid*, pg 30, line 1092.
[15] *Ibid*, pg 30, line 1083.
[16] *Ibid*, pg 33, line 1155.

- On page 11, line 374, the NSTAC recommends that the EOP replace "convenience" with "enablement." Research has repeatedly shown that improved convenience in performing existing tasks does not change public behavior or lead to commitment to buy or embrace new technology. On the other hand, use of such technology to facilitate expanded functionality in new dimensions does change behavior and user attitudes. Enablement of completely new capabilities for general users is a powerful, positive feature latent in the NSSOT and its emphasis will aid and accelerate acceptance.