From: Richard Lamb <slamb@xtcn.com>
To: nsticnoi@nist.gov
Date: Aug 5, 2011
Subject: Docket Number 110524296-1289-02

5 August 2011

Annie Sokol
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

Via email: NSTICnoi@nist.gov

Reference: Docket Number 110524296-1289-02

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

Dear Ms. Sokol

With reference to your announcement in the Federal Register, as my feedback is outside the response period I do not expect any consideration. However, given the nature of the last question I feel I may have something to contribute from my recent experiences in successfully deploying an authentication platform amidst a similarly wide range of policy and technical challenges[1]. To this end I would like to provide comments on question 4 that you may take or leave given the lateness of my response. I hope in some small way this is helpful.

4.1 As you correctly point out, although this is a US effort, the borderless nature of the Internet requires any meaningful identity system to take into account international usage. To this end, the structure of the steering group should encourage cooperation by A) surveying similar foreign efforts – both mature and in development[2]; and B) regularly inviting and exchanging presentations from such efforts.

This is critical as it allows the NTSIC effort to bootstrap from the lessons learned from these efforts and avoids reinventing the wheel. Inclusion and involvement also encourages cooperation and a pathway to interoperability. While I am cognizant of the differences in national laws (e.g. privacy regulations) and requirements, some of these efforts have struggled with the same issues we are.

[1] I was ICANN’s technical and policy architect for deploying DNSSEC at the root of the Internet’s domain name system (DNS) July 2010. This not only opened the door to digital authentication of the Internet’s phone book (the DNS) but also allowed for a single framework for a global PKI that will allow for various authentication mechanisms to be linked and work across organizational and national boundaries. This required a carefully implemented transparent multi-stakeholder approach that built in international involvement.

[2] Swedish e-ID program: http://www.kirei.se/2009/10/19/eid-i-sverige/ Google Translate does a reasonable job here. From ministry of finance:
http://www.regeringen.se/content/1/c6/15/82/56/74c79ddf.pdf
Estonia ID: http://en.wikipedia.org/wiki/Estonian_ID_card

Similarly, the steering group should draw on the experience multi-national vendors that have already obtained regarding the regulations in various nationalities in order to promote and sell their products. This should also provide a short cut and short circuit bureaucratic processes that would delay useful deployment of the Strategy.

In concert with the above, once a baseline framework and strategy has been agreed upon, the steering group should reach out to international organizations such as ISO to inform them of our progress while not relying solely on their input or holding up our efforts.

4.2 Regarding coordination. Experience on the very same Internet we hope to fortify with NSTIC has shown the value of the bottom-up development process (e.g., in protocols like tcp/ip, dns, dnssec) over the top down intergovernmental approaches (e.g., X.500/OSI, ICAO e-passports). The same lessons should be applied here, i.e., informal discussions with our counter parts in various governments (possibly with assistance from vendors for introductions), sharing knowledge in the form of informal face to face presentations and gatherings. Similarly for the technical aspects: it is best to start from the ground up by building on the international, de-facto standards and products that are already being tracked and followed between engineering groups (e.g., RSA PKCS and ISO smart card standards).

To foster this, interoperability demonstrations should be first on the technical agenda along with policy development in parallel. (I would expect the steering group to split up into at least technical and policy working groups.)

4.3 Focus should be in drawing lessons and experience from existing industry led international efforts combined with existing international initiatives – government or private sector (e.g., FedPKI, CAs, OpenID) – not necessarily only on standards bodies where efforts can often get bogged down. Finally, a survey of efforts from international standard setting organizations that incorporate broader public policy concerns such as ICAO, ICANN, etc should be completed.

4.4 As stated above, interoperability demonstrations should be the first on the list of goals. The steering group should make this the first goal by selecting a date, say 9 months from now, for various approaches and technologies to come together. Such an event should be accompanied by multiple networking opportunities to informally exchange approaches and ideas.

Not to be dismissed is the natural propensity of many governments to follow US efforts in IT security (e.g., FIPS, encryption standards). Inter-operability bake-offs would be an opportunity for them to not only see what will be coming down the road but to effect that direction by being involved in the process.

Having similar inter-op sessions or at minimum, public awareness building sessions at high profile internationally attended industry conferences such as RSA is also critical to ensure no one is taken by surprise when standards are proposed for adoption.

4.5 USG serves a critical role here facilitating, providing a leadership role, and its imprimatur to the efforts in this ID ecosystem. The government centric nature of IT efforts in many other countries require that in order for the results arising out of NSTIC to be taken seriously (and have hope for some level of international interoperability) this effort should be viewed as having the imprimatur of the federal government. However, USG should not be seen to define the specific protocols or underlying technology in this ecosystem lest unwarranted suspicions arise from conspiracy theorists. In that respect, from the start it should be assumed that not all nations will embrace cooperation nor become fully interoperable with a US based ID system.

Key here is being open to the optional involvement by other nations and showing a willingness to collaborate on mutual recognition agreements of indigenous national standards once winners in the global ID ecosystem eventually arise.

This feedback is solely my own and should not in any way be construed as the opinions of my employer. Thank you for taking on such a timely and critical effort. If you have any questions please do not hesitate to contact me.

Dr. Richard Lamb
Internet Beneficiary