MAAWG

From: Messaging Anti-Abuse Working Group (MAAWG)
Date: July 19, 2010
Subject: Comments on the National Strategy for Trusted Identities in Cyberspace

Thank you for the opportunity to review and comment on the National Strategy for Trusted Identities in Cyberspace (http://www.dhs.gov/xlibrary/assets/ns_tic.pdf).

The Messaging Anti-Abuse Working Group is an international non-profit industry-lead organization founded to fight all forms of abuse, such as phishing, botnets, fraud, spam, viruses, and denial-of-service attacks. Drawing technical experts, researchers and policy specialists from a broad base of Internet Service Providers and Network Operators representing over one billion mailboxes, key technology providers, academia and volume sender organizations, MAAWG's (www.MAAWG.org) multi-disciplinary approach includes education, advise in public policy and legislation, development of industry best practices, guidance in development of industry standards, and facilitating collaboration. Scalable, secure, and trustworthy identity and privacy are pivotal to our work.

We are, therefore, pleased to see the administration's interest in developing and deploying a national strategy for trusted identities in cyberspace, and we would like to share some comments reviewed and approved by the MAAWG Board of Directors regarding that strategy.

In general, MAAWG is supportive of the NSTIC draft as written, although we recognize that this is just a draft plan, and will likely evolve as a result of comments you receive. Obviously, if the current draft changes in material respects, that may improve or diminish our ability to support future versions.

As currently written, however, we see much that we like. For example, we believe the nine actions mentioned on pages 2 and 3 of the draft are appropriate, necessary and worthy of support. Similarly, we also believe that the eight guiding principles outlined on pages 8 through 11 are also sound.

At the same time, we do have some areas of concern:

1) For a project of this importance and potential magnitude, an initial pilot scale implementation will likely yield important insights, and may offer an opportunity to identify issues or to refine the approach that will be ultimately deployed in production. We view deployment of a pilot scale demonstration project as time that would be well spent, even if it briefly delays the availability of a national scale production identity infrastructure.

2) Much work has already been done in federated identity and privacy preserving authentication. Projects that particularly come to mind in this respect include the work on OpenID (http://openid.net/), Shibboleth (http://shibboleth.internet2.edu/) and the InCommon Federation (http://www.incommonfederation.org/). If the NSTIC is able to leverage the output of those initiatives, NSTIC may be able to take advantage of lessons already learned, including experience with multi-million-user production federated identity deployment efforts.

3) Trustmarks are widely referred to in the draft document as an important end-user signal. While there is value to the simplicity that a simple binary "certified/not certified" brings, a more finely nuanced

rating (such as a numerical score, or an A to F grade), may give users more information with which to evaluate their options, and may encourage providers to do more than if they were simply striving for at least a minimally satisfactory grade on a "pass/fail" scale.

4) The NSTIC's work should also insure that we move beyond traditional passwords. Passwords are under continual attack, and ultimately will need to be augmented or replaced by something more secure, such as hardware cryptographic tokens, biometric methods, certificates, two channel approaches or a combination thereof. The NSTIC should emphasize that important objective.

5) Some technologies mentioned in the draft, such as IPSEC, DNSSEC, and BGP security (see pages 15-16 of the draft report) have had limited production uptake to-date. If those technologies are critical to the success of the NSTIC, their limited deployment to-date would be an obstacle.

6) Revocation of credentials has traditionally been a tricky issue for identification infrastructures (such as PKI deployments), and is an issue that has been dealt with imperfectly to date. It will be important for us to get revocation-related issues right for the purposes of NSTIC, and neither revocation lists nor OCSP (online certificate status protocol) represent a wholly satisfactory option. More work is needed in this area.

7) We need to learn from the problems we've experienced with registrars and the domain name system. In particular, when we take note of the over one hundred proposed modifications to the current ICANN Registrar Accreditation Agreement (see http://gnso.icann.org/issues/raa/report-raa-improvements-proposal-28may10-en.pdf), it's clear that constructing a global scale and secure commercial Internet infrastructure is non-trivial. As we look at deploying yet another national or global scale Internet infrastructure, we need to insure that all providers accredited to this new identity initiative are fully worthy of participant trust and confidence, and are held to the highest technical and operational standards for availability, integrity, transparency, and fidelity.

8) Another requirement is the need to protect the privacy of law-abiding users while simultaneously insuring that cyber criminals can be successfully "decloaked" following established legal process. That is, we need "assured privacy" with "enforceable accountability," thereby insuring that user privacy is maintained while simultaneously preventing online abuse and cyber crime. We recognize that balancing these two seemingly mutually contradictory requirements is difficult, but anything less than an appropriately balanced solution will likely deter adoption and be unacceptable to one part or another of the larger Internet community.

MAAWG would like to thank you for the opportunity to submit these comments for your consideration, and we would welcome the opportunity to offer further assistance to the administration on its work in this important area. Please feel free to contact us if you have any questions, or if we can be of any further assistance.

Sincerely,
/s/
Jerry Upton
Executive Director
Jerry.Upton@maawg.org