

Comments on Draft of National Strategy for Trusted Identities in Cyberspace

(http://www.dhs.gov/xlibrary/assets/ns_tic.pdf)

U.S. Public Policy Council of the Association for Computing Machinery

July 19, 2010

On behalf of the U.S. Public Policy Council of the Association for Computing Machinery (USACM), we submit the following comments in response to the Department of Homeland Security's request for comments about the Draft National Strategy for Trusted Identities in Cyberspace (Draft Strategy).

With over 94,000 members worldwide, the Association for Computing Machinery (ACM) is an educational and scientific society focused on advancing computing as a science and a profession. USACM serves as the focal point for ACM interaction with U.S. government organizations, the computing community, and the public in all matters of U.S. public policy related to information technology. Should you have any questions or concerns, please contact Cameron Wilson at our Public Policy Office, 202-659-9711.

Authentication and attribution of identity are not among our most critical cyber-security issues

Because authentication and attribution of identity does not help with most of the pressing cyber-security issues we face today, the Draft Strategy is unlikely to make a significant impact on the state of cyber-security. A recent hearing of the Technology and Innovation Subcommittee of the House Science and Technology Committee¹ highlighted the challenges of proper attribution and the potential for exploiting those challenges. The USACM paper on Understanding Identity and Identification² highlights how misunderstandings over authentication and identification complicate security.

A more pressing concern in cyber-security (as demonstrated by the nature of many recent data breaches and security compromises) is ensuring that underlying information technology is effectively secure and resistant to malicious software ("malware") of various types. Strong identification will not compensate for information technology that is poorly designed, configured, and/or operated. Indeed, vulnerabilities in the underlying technology will threaten the integrity of such a scheme. Greater efforts aimed at more effectively securing information technology, moreover, would also emphasize prevention rather than response.

This raises serious questions about the value proposition represented by the Draft Strategy, which will entail significant monetary costs, as well as potentially significant negative privacy and security impacts (in addition to the potentially positive ones). If the strategy is broadly implemented, as currently envisioned, it is unlikely to deliver a proportionate level of benefits for the costs and negative impacts involved. The experiences of commercial efforts such as those of Liberty Alliance raise doubt about the viability and value of a national identity infrastructure. By the same token, the feasibility of an

¹ http://science.house.gov/publications/hearings_markup_details.aspx?NewsID=2874

² <http://www.acm.org/usacm/Issues/identity.pdf>

effective national strategy in the context of a global Internet is also questionable. However, a much more focused effort aimed at critical infrastructure and government functions might prove worthwhile.

Centralized, nationwide information management can introduce vulnerabilities and thus undercut the goals of the strategy

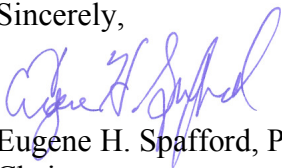
The Draft Strategy may indeed help privacy concerns in some respects, but the relatively centralized maintenance of identities and associated attributes introduces new risks that undercut potential benefits. A single certified online identity raises the value of that identity, making it more tempting to steal and harder to recover. This is a problem for any system, such as REAL ID, that places too much faith in a single credential. The Draft Strategy also underestimates the challenge of effectively implementing Fair Information Practice Principles and ensuring compliance with those principles. For example, enabling selective attribute disclosure and ensuring that a relying party requires disclosure of only genuinely necessary attributes are two entirely different things. Allowing for multiple independent identities (as opposed to just pseudonyms linked to the same identity) for different purposes and/or domains would reduce the risk of identity theft and increase the privacy of users without imposing significant expense; however, this is not currently part of the Draft Strategy.

Mission creep would make a ‘voluntary’ program effectively mandatory

The Social Security Number (SSN) was originally intended to identify individuals for the purposes of tracking a person’s contributions and benefits over time. Today the SSN is widely (over)used for all kinds of purposes inside and outside of government. Many identity theft cases deal with fraudulent financial transactions because of the relative ease of obtaining someone else’s SSN. We are concerned that what is called for by the Draft Strategy, even though individual participation is voluntary, would become a requirement for nearly everything online, even services that gain no appreciable benefit from having the identity of one or more participants certified. Again, a more focused effort would be preferable to what is being proposed.

Thank you for considering our comments. We look forward to a continued dialog with you as the draft strategy moves forward. If you have any questions, please feel free to contact us directly, or through Cameron Wilson, Director of Public Policy for ACM.

Sincerely,



Eugene H. Spafford, Ph.D., D.Sc.
Chair
U.S. Public Policy Council of the
Association for Computing Machinery



Stuart Shapiro
Chair
Security and Privacy Committee
USACM