INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

The Honorable Patrick Gallagher
Under Secretary of Commerce for Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Dr. Gallagher,

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

At the Board meeting of November 3-5, 2010, Board discussed usability and security with a panel of experts. The panel addressed topics including password use, intersection of government authentication with what people use in their daily lives, complexity of explanations for current security regimes, and lack of understanding by users of implications of poor security. In addition, the Panel discussed current challenges, including:

- Cognitive limits on number of passwords
- Externalities
- Ability to get around/opt-out
- Lock-outs that limit use and frustrate ecommerce take-up

At the same meeting, the Board also heard from an expert on the National Strategy for Trusted Identities in Cyberspace (NSTIC) about their activities. Much of the successful implementation of NSTIC depends on implementation of good security measures by government, industry, and citizens as they establish online identities to exchange information and conduct business over the Internet. This element of the NSTIC would benefit from a strong research program that addresses usability issues like those being pursued by NIST and industry. Such research would be advantageous from several different dimensions:

- Near-term: how to facilitate more effective and broader use of existing credentials for authentication in interacting with government online.

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007

- Mid-term: how to incentivize industry, especially critical infrastructure sectors, to implement easy-to-use but strong authentication that leverages both government and commercial activities

- Long-term: how to make citizens understand the value of using good security for authentication, while also working with product companies to develop simple and transparent processes for individuals to follow in practicing good security

Based on the discussions heard by the Board, goals for a research program to support NSITC could include:

- Developing "mental models" of how users incorporate security in their online identities, taking into account the results of behavioral research

- Quantifying in a clear and recognizable way the harm that comes from poor security, and communicating that harm in meaningful ways

- Framing a metaphor that explains individual connection with a complex online identity eco-system, which can incentivize what government, industries, and individuals can do to act more effectively

The Administration has taken a significant step forward toward the implementation of NSTIC with the establishment of the National Program Office within Commerce. The Board understands that NIST continues to play a key leadership role as part of the NGO, and recommends that this strong and well-supported role be leveraged to promote a research element for NSTIC that incorporates the views outlined above – NIST has led much of the work on developing a national consensus on a variety of key issues in cybersecurity, and encryption and can build on current research and identify management programs.

The Board appreciates the opportunity to provide our views.

Sincerely,

Daniel J. Chenok
Chair
ISPAB

cc: The Honorable Gary Locke, US Department of Commerce
Vivek Kundra, Administrator of E-Government and Information Technology and CIO, OMB
Howard Schmidt, Cybersecurity Coordinator, National Security Council