INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

OCT 20 2009

Ms. Cita Furlani
Director, Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Dear Ms. Furlani,

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.

On October 7, 2009, the ISPAB met with you in a special one-day meeting under the Federal Advisory Committee Act (FACA) to discuss the proposed reorganization of the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST). Specifically, the Board addressed those elements of the reorganization that would impact the Computer Security Division (CSD) and NIST's overall role regarding Federal agency information security. The meeting resulted from a discussion of this issue at the ISPAB meeting of July 30, which immediately followed initial reports that an ITL/CSD reorganization was being considered, followed by a request from your office for a follow-up discussion by the Board.

The Board heard from a number of members of the public during this session, including former CSD leaders, industry experts, and a former ISPAB member. We then engaged in a wide ranging discussion with you about the goals and objectives of the proposed reorganization. In the end, the Board voted unanimously to communicate our advice to you through this letter, copies of which are being sent to the Deputy Director of NIST, the Secretary of Commerce, and the Director and the E-Government Administrator in the Office of Management and Budget.

The Board greatly appreciates the open and candid exchange of views that occurred at the October 7 meeting. We commend you and NIST for the willingness to expose the proposed reorganization to public review through the FACA process.

Based on our meeting and the input from members of the public, the Board draws a number of findings regarding the proposed reorganization given the increasingly vital and visible role of cybersecurity to achieving Government missions.

- NIST continues to play an important leadership role for Federal agency computer security. NIST guidance provides the basis for technical, operational, and managerial steps necessary for appropriately securing information assets; NIST experts are widely respected for their assistance to agencies; and NIST is a key link between legislation, OMB policy, procurement, and agency day-to-day protection.

- NIST links with the Department of Homeland Security and the intelligence community on an increasingly frequent basis to ensure consistency across the civilian, law enforcement, and classified security arenas.

- Industry views NIST as a key Federal partner. NIST provides a neutral, non-classified environment for industry to make their views known to the Government; NIST takes industry input seriously in formulating its guidance; and this guidance influences industry activity more broadly as industry often voluntarily adopts NIST precepts as best practices for their non-government security business as well.

- NIST participates in international security fora as the US lead representative, providing an international standards perspective that is highly valued by industry. Both foreign governments and international organizations work with NIST regularly in developing cross-border approaches to security.

- In all of the above areas, the Computer Security Division has been the home for the vast majority of NIST's information protection activity. CSD houses expertise and experience, and enjoys broad recognition and respect. Perhaps most importantly, CSD has developed a renowned "brand" due to its success for over the past 20 years.

- NIST may wish to discuss any substantive reorganization of its Federal agency computer security program with the White House Cyber Coordinator once that person is in place, so that the Coordinator may review NIST"s role and responsibilities within the overall Federal security program -- including how the current and proposed NIST/CSD organization aligns with recommendations in the President's 60-Day cybersecurity review.

At the same time, the Board recognizes that protecting Federal assets is an evolving challenge, needing periodic review of organizational structures to ensure that resources are allocated to maximize the impact of policy and guidance. We also have noted in the past, and reinforced in the October 7 meeting, that NIST's effectiveness could be enhanced in a number of ways – for example, CSD could do more outreach to improve the understanding of basic security measures by non-technical users, and could increase its attention to privacy controls as a critical and complementary discipline to security. Any potential reorganization should seek to retain strengths, close gaps, and – perhaps most importantly – be flexible enough to adapt and support evolving future needs for cybersecurity in government and industry.

The Board shares your objectives to elevate and strengthen NIST's role in carrying out its statutory responsibilities for computer security, and agrees that this important function deserves attention across ITL and the Director level. In this regard, we offer the following recommendations that are intended to provide context for the specific actions that you take in any reorganization.

- Any reorganization of computer security responsibilities in NIST should strengthen its ability to set standards, guidance and leadership for Federal agencies. A change should also enable future expansion of the NIST security program, should this be authorized and properly resourced. The ISPAB offers two options for accomplishing this, based on several public and Board member comments:
    - To reflect the importance of security across ITL, consider identifying security as part of the Lab's overarching purpose -- for example, by including it as part of the Lab's name.
    - Given the increasing importance of cybersecurity across many Federal missions, consider elevating CSD on its own to the Lab level.

  Should NIST not pursue the second option of a Cybersecurity Lab at this time, the increasing importance of cybersecurity across many Federal missions may warrant renewed consideration of this step in the future.

- We concur with the proposal for an Associate Director for Cybersecurity as a direct report to the ITL Director, and recommend that this office be provided substantive authority to influence NIST activities in this area as opposed to simply coordinating such activities; such authority would require that appropriate resources be given to the function.

- The resources devoted to cybersecurity should ideally be maintained in a single organization with a recognized "brand", as with CSD. However, should other factors justify spreading current responsibilities across more than one division, the Associate Director for Cybersecurity should ensure strong coordination among those divisions.

- Restructuring ITL's responsibilities in this area should also account for the increasing attention to information privacy as another element of cyber protection for the Federal government. There is no privacy institution similar to the role NIST plays for security. An enhanced role for ITL in promoting strong protection for personally identifiable information, and for the broader privacy characteristics including transparency, consent, access, would be of great benefit to the Government.

The Board appreciates the opportunity to provide our views to you. We hope that our discussion in the meeting on 10/7, and the advice contained in this letter, help you to frame a strong approach for NIST in fulfilling its cybersecurity mission and serving the many stakeholders who rely on NIST for guidance.

Please let me know if you would like more information from the ISPAB on these issues.

Sincerely,

Daniel J. Chenok
Chair
ISPAB

cc:
The Honorable Peter Orszag, Director, OMB
Vivek Kundra, Administrator of E-Government and Information Technology and CIO, OMB
The Honorable Gary Locke, Secretary, Department of Commerce
Patrick D. Gallagher, Deputy Director, NIST