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 Jeffery Zients
Acting Director
U.S. Office of Management and Budget
Washington, DC 20502

Dear Mr. Zients,

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 our meetings of April 7 and August 4, NIST staff briefed the Board about its assumption of leadership for this Initiative 8 of the Comprehensive National Cybersecurity Initiative, regarding Cyber Education – a vitally important element of the Administration's overall cybersecurity strategy. The White House web site summarizes Initiative 8 as follows:

> In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge.

The Board strongly supports NIST taking on this role, which complements existing security education and awareness activities of the Computer Security Division, and integrates security understanding and skill development with the Government's lead entity for technical security content. The Board recognizes that NIST's coordination is underway, and looks forward to working with NIST as this initiative develops.

During the course of the discussion and in follow-up deliberations, the Board identified several issues that we believe would be important for NIST to address with OMB, DHS, and other interested stakeholders, in order to maximize the effectiveness and impact of this activity. Specifically:

> Most of this focus area appears to address developing skills in the Federal workforce, which is a critically important objective. However, most Federal information security services are provided by contractors. We believe that the initiative should identify skill

needs and training opportunities that would be applicable to both government and industry, as well as academia, in order to bring its benefit to all involved parties. We would recommend that NIST reach out to industry associations, including those that represent critical infrastructure sectors, to collaborate in this arena.

- There is less need to classify information pertaining to cybersecurity workforce skill needs and training than for other elements of cybersecurity. In addition, greater understanding of skill requirements will allow schools to properly frame their educational offerings, and will incentivize contractors to hire for skills that match those requirements. Accordingly, we encourage further declassification and transparency in the cyber education and awareness arena to the maximum extent appropriate balancing needs for national security.

- At the present time, NIST's role on the initiative appears to be more of a coordination function than a decision making role. We would recommend that the Administration bring NIST into resource allocation and decision processes as appropriate, so that resource decisions reflect agency needs as reported by NIST. We would also recommend that the resources available to NICE stakeholder agencies to operate the program be sufficiently robust to allow for sustained attention over time.
Emerging/Managerial/Technical/Administrative issues relative to information security as it pertains to……

These initial recommendations are intended to help NIST, OMB, and the Administration in addressing certain gaps to enhance the chances for success at the outset of its leadership for this key national program.

The Board appreciates the opportunity to provide our views.

Sincerely,

Daniel J. Chenok
Chair
ISPAB

cc:
Vivek Kundra, Administrator of E-Government and Information Technology and CIO, OMB
Howard Schmidt, Cybersecurity Coordinator, National Security Council
Patrick Gallagher, Director, NIST