INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

ESTABLISHED BY THE COMPUTER SECURITY ACT OF 1987 [Amended by the Federal Information Security Management Act of 2002 And the Federal Information Security Modernization Act of 2014]

July 20, 2017

Dr. Kent Rochford
Acting Undersecretary of Commerce
for Standards and Technology
Acting Director, National Institute
of Standards and Technology

The Honorable Mick Mulvaney
Director of the Office of Management
and Budget
725 17th Street, NW
Washington, DC 20503

Dear Dr. Rochford and Mr. Mulvaney,

I am writing you as the Chair of the Information Security and Privacy Advisory Board (ISPAB or "Board"). ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-235) 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 Management Act (FISMA) of 2002. The statutory objectives of the Board include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to federal information security and privacy. The Board wishes to communicate to you the following:

Maintaining Current NIST Authorities

As a federal advisory board, ISPAB was created to track and advise on both the progress of federal information security management and NIST's role in supporting that progress. To meet this support function, NIST was vested by the Computer Security Act with "honest broker" authority to convene federal and private sector stakeholders to develop consensus-based cyber security standards of practice and guidance. The result has been widely adopted cybersecurity guidance such as the 2014 Cybersecurity Framework and the extensive "800-series" guidance documents. This impartial, "big-tent" approach has earned the agency its reputation and respect in the cybersecurity community, with broad agreement that the partnership model works.

One role not statutorily vested with NIST is an information security audit function. Recent proposals to expand NIST's purview with audit authority over federal agencies could compromise NIST's hard earned reputation as a trusted and effective honest-broker in the cybersecurity community. Even if this authority were restricted to federal agencies, private sector stakeholders might be less inclined to collaborate with NIST if they suspect its guidance could later become a regulatory standard with compliance requirements.

Moreover, requiring such a new authority of NIST would likely distract the agency from its core mission of standards and guidance development and research, and force the agency to reallocate resources away from those functions.

The Board observes that every federal agency with an inspector general (IG) function should, pursuant to the Inspector General Act of 1978, rely on its in-house expertise to conduct information security audits in alignment with appropriate NIST guidance. Oversight of this process is vested in OMB as stipulated in the Federal Information Security Management Act . Audit authority therefore already exists, but is inconsistently exercised across the federal enterprise. The Board recognizes that many agency IG's lack the necessary expertise to perform meaningful and conclusive information security audits because of the technical and constantly shifting nature of cybersecurity threats and mitigations.

Accordingly, the Board recommends that greater attention be devoted to training IG's on federal information security requirements, and potentially on appropriate methodologies for conducting information security audits. Developing this kind of training and advisory role would be a more appropriate augmentation of NIST responsibilities than would a new, untested and un-resourced audit authority. A cyber training strategy would, in addition, facilitate agencies' fulfillment of the information security risk management requirements enumerated in Section 1(c) of Presidential Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."

NIST's Privacy Engineering Program

NIST's Information Technology Laboratory (ITL) has been a thought leader in developing the concepts of privacy engineering and risk management for federal systems. These efforts have facilitated a better understanding and communication of privacy risk within federal systems, and helped define implementation of broadly accepted privacy principles.

In January 2017, NIST's NISTIR 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems, provided the basis for two innovations -- the application of privacy engineering as a discipline and a privacy risk management model. At the ISPAB's June meeting, NIST staff expressed the positive reception that privacy engineering is receiving from federal agencies and the private sector. NIST is considering as a next step how to improve its privacy risk assessment methodology and make it and other privacy engineering tools more widely available for use. Currently the methodology is a manual process, so having better

automated tools could enable entities to more easily and effectively conduct their assessments and then implement technical and policy measures to mitigate their privacy risks.

The Board urges the Administration to support efforts to build a privacy engineering toolkit collaboration space that would draw technical and policy experts from academia, private sector, and government to explore development of tools to implement NIST's methodology. This collaboration would spark innovations to achieve greater privacy protections and accountability, ultimately furthering the overarching and challenging goal of "Privacy by Design."

Christopher Boyer
Chair
Information Security and Privacy Advisory Board