INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

December 09, 2021

Dr. James Olthoff
Performing the Non-Exclusive Functions and Duties of the
Undersecretary of Commerce for Standards and Technology &
Director, National Institute of Standards and Technology

Dear Dr. Olthoff,

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. 100-235) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, and The Federal Information Security Modernization Act (FISMA) of 2014. The statutory objectives of the Board include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

In December 2020, the ISPAB sent a letter to Dr. Walter Copen, then the Undersecretary for Standards of the Department of Commerce, regarding the resourcing of the privacy program at NIST. The ISPAB has not received a reply to that letter, and given the change in Administrations, we are concerned that our recommendation may have been overlooked during the transition. This letter repeats our previous observations and recommendations.

It is clear to the ISPAB that issues relating to privacy and the collection, creation, use, analysis, and sharing of personally identifiable information (PII) continue to increase at a rapid pace as the government embraces new, innovative technologies and new sources of PII, many of which are unknown to individuals, are developed. Over the past decade NIST has developed a program to address privacy issues along with NIST's myriad other programs in cybersecurity.

As you are aware, the goal of NIST's privacy initiatives is to help data-driven organizations innovate and derive benefits from data while simultaneously managing risks to individuals' privacy. The cornerstone of NIST's work is the NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, which was released on January 16, 2020. The Privacy Framework provides a common language for understanding, managing, and communicating privacy risk with internal and external stakeholders. NIST also pursues numerous related efforts in privacy that seek to equip federal agencies to conduct privacy engineering, assess and manage privacy risk, and develop a privacy workforce.

This critical and groundbreaking work in the field of privacy supports NIST's efforts to promote trustworthy systems and complements the widely adopted NIST Cybersecurity Framework. The

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

significance of NIST's work is amplified by the Office of Management and Budget's July 2016 update to OMB Circular A-130, which requires federal agencies to apply the NIST Risk Management Framework to agency privacy programs. This new mandate increases the importance of the NIST role in developing practical tools to support agency efforts to operationalize privacy requirements, evaluate privacy risk, implement privacy controls, and develop repeatable and measurable processes to protect Americans from potential adverse consequences related to processing their personal data. This work is essential.

At our October 2020 meeting the ISPAB learned that the privacy program at NIST has a total of only 4 FTE. The work that NIST has been able to produce with only 4 FTE is extraordinary but the ISPAB is concerned that 4 FTE will not be adequate to address the growing demand for privacy talent and privacy guidance in light of rapidly evolving issues and technologies such as machine learning, digital identity, cloud computing, autonomous vehicles, precision medicine, and online engagement. We recommend that additional resources be identified and applied to the NIST efforts to advance privacy risk management and privacy engineering and develop a privacy workforce so that agencies can meet the privacy challenges of the future and maximize the benefits of technology while simultaneously managing the risk of adverse consequences to individuals and society.

I am available and happy to speak with the staff or individuals responsible to further discuss the board's insights and concerns.

Thank you very much.

Sincerely,

Steven B. Lipner
Chair
Information Security and Privacy Advisory Board