INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

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.

At its meeting on 3 March 2021, the Board heard forensics brief on the SolarWinds intrusion. The timeline of the SolarWinds intrusion indicated that that the attackers had slowly and patiently executed this attack and remained undetected over the course of a year. Secure cloud software and network configurations could have mitigated the attack; however, network defenders— faced with overly large networks, insufficient trust models, and out of date risk management procedures—are unable to develop and distribute secure configurations for all the software on their networks in timely fashion. This challenge will limit their ability to prevent the next such intrusion.

Because it is impossible to know the target of the next intrusion with a large security impact like SolarWinds, the U. S. Government needs a timely and scalable solution for implementing secure configurations on their networks. Interrelations between government and private networks imply that secure configuration solutions should be available to the public as well. The Board recommends that NIST and DHS develop technical approaches for products that are configurable to ensure that they are secure and useable as well as incentivization strategies to ensure that secure configurations are supported by product developers and implemented by users. Machine-readable expressions of secure configuration guidance are preferable to automate network security; the Board is working on a broader recommendation regarding automation, and machine-readable configuration settings are likely to be an element of that recommendation.

The Board recommends that NIST and DHS create policies and guidelines as appropriate to support the realization of these incentivization approaches, and that they work with agencies and private sector

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

organizations with relevant technical expertise in the development of incentivization and policy updates. This collaboration should include the identification of areas in which the promulgation of secure configurations would benefit the security of government systems and evangelization for secure out-of-the-box configurations to the vendor and Federal user community for their adoption. Promulgation and evangelization efforts should target initial configuration settings development as well as configuration updates as threat information becomes available.

The Board also recommends that OMB develop requirements that agencies use vendor-provided secure-out-of-the-box configurations and configuration updates on government networks wherever feasible.

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

CC: Secretary Mayorkas, United States Department of Homeland Security,
Shalanda D. Young, Acting Director, Office of Management and Budget