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 briefings on the SolarWinds intrusions, the effectiveness of security compliance programs, and the security issues associated with Open Source Software (OSS). One consistent thread that ran through these briefings, as well as other briefings that the Board has received at previous meetings, is that system designers and software developers are not doing an adequate job of considering security as they create or modify systems and software. This problem affects both systems that are developed for government use and commercial and OSS products and services that government consumes as a customer.

The Board believes that inadequate consideration of security results in large part from designers and developers having insufficient security education and training. They are too often unaware of the security consequences of their work and consider security to be a problem that the security organization should address after the system and software are built. Unfortunately, once a system or software product has been created without adequate attention to security, remediating its problems is costly in time and money, and too often the needed work gets delayed or ignored.

To address this problem, and to improve the security of the systems and software on which the United States relies, the Board recommends that the National Initiative for Cybersecurity Education (NICE) should work with education and training providers to ensure job-appropriate security education and training is available for the broad population of system designers and software engineers. This education and training should be aligned to the Workforce Framework for Cybersecurity (NICE Framework) to enable designers and developers to create systems and software whose security is built in. Some

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

commercial vendors have provided this sort of education and training to their development staffs and found that it pays significant dividends in terms of improved security and reduced need for after-the-fact remediation. Such training of the broad development population does not eliminate the need for cybersecurity personnel whose purpose is to protect and defend data, systems, software, and online services to minimize the cybersecurity risks to organizations rather, it makes their efforts more scalable and effective. The provision of such training is an effort well worth undertaking, and NICE is well-positioned to guide that effort for the United States Government. The Board believes that training system designers and software developers in security will be most effective as IT modernization is pursued across the government since it will enable the government to avoid diminishing returns that can result if developers attempt to embed new cybersecurity techniques into old architectures and infrastructure.

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