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 a briefing on a recent study of the security practices of developers of Open Source Software (OSS) and on a new nonprofit organization, the Open Source Security Foundation (OSSF), that has been created to improve the security of OSS. OSS is software that is typically created from the contributions of a wide range of developers, some paid and some unpaid, and made widely available for individuals and organizations to use and modify as they see fit. The U.S. Government and the contractors that support it are major consumers of OSS, and OSS is built into many systems and online services on which the government relies.

Given the lack of widespread security education among developers, especially developers who are not associated with organizations that have mature software security processes, the security of OSS can vary widely. Some OSS components have suffered serious vulnerabilities that affected their user organizations. The recent survey of OSS developers by the Harvard Business School confirms that few OSS developers have interest in or commitment to the processes that are necessary to create secure software. The Linux Foundation, in collaboration with a number of major organizations that are committed to the use of OSS, has established the OSSF to address the challenge of OSS security by improving developer awareness and training, and by providing resources such as tools and security audits that OSS projects can adopt.

As a major consumer of OSS, the U.S. Government has a significant interest in the security of OSS and shares the goals of the OSSF. For this reason, the Board recommends that the director of NIST, in his role as Undersecretary of Commerce for Standards, strongly encourage that government agencies or contractors that depend on OSS join the OSSF and support its efforts to improve the security of OSS for all users.

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