

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

May 15, 2023

Dr. Laurie E. Locascio
Undersecretary of Commerce for Standards
Management and Technology
Director, National Institute of Standards
and Technology

Dear Dr. Locascio:

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.

On March 2, 2023, Allan Friedman, Senior Advisor and Strategist, Cybersecurity and Infrastructure Security Agency (CISA), provided the ISPAB, with an update on Software Bill of Materials (SBOM) activities for federal agencies.

The ISPAB supports and commends the Administration's ongoing and increasing efforts to address the relentless and increasingly sophisticated cybersecurity threats our Nation faces.

This commitment includes recent actions to improve the security and integrity of the software supply chain through initiatives such as SBOM.

ISPAB notes that there are two primary use cases associated with SBOM. The first use case concerns development organizations (developers and suppliers of software products and services or open-source projects) who must know what software they are incorporating in products or services to prevent, identify, and respond to vulnerabilities and supply chain incidents. This use case is a fundamental part of the NIST Secure Software Development Framework and is well-established in secure development programs going back almost twenty years.

The second use case involves a different set of stakeholders: the use of SBOM by end user organizations that purchase, deploy, and operate software, including government agencies. This

use case is intended to help end user organizations track and respond to vulnerabilities. and is mandated by Executive Order 14028, "Improving the Nation's Cybersecurity."

The ISPAB supports efforts to identify and inventory the components of software products and services. The ISPAB notes however, that the consumption and exploitation of an SBOM may be a resource-intensive endeavor and we have concerns that government agencies tasked with consuming SBOM may not currently have a reliable measure of the utility, efficacy, and cost-effectiveness of SBOM.


The ISPAB understands that the wide-scale adoption of SBOM is an ongoing initiative and that NIST, CISA, NTIA and other stakeholders have identified further work. As part of these ongoing efforts, ISPAB recommends that CISA and NIST jointly document intended functions of SBOM for government agencies acquiring and operating software and develop quantitative metrics to evaluate success based on intended functionality. Success of SBOM initiatives should not be measured based on adoption rates, which may provide a false sense of security and impact. Instead, the Board believes it is important to specify precisely how SBOM is intended to improve the cybersecurity posture of agencies, and devise metrics to evaluate whether SBOM achieved the desired results and outcomes. For example, can agencies determine if SBOM reduces time to incident response? Does SBOM demonstrably improve Federal incident response? Have any agencies successfully completed a trial or table-top incident response leveraging SBOM and if so, can the results be shared broadly to inform the evolution and adoption of SBOMs?

The ISPAB commends the Administration's ongoing efforts to address cybersecurity. One of our objectives is to offer practical guidance to support and improve this critical work. With respect to SBOM, we believe that the development and use of quantitative, outcome-based metrics is essential, both to evaluate the efficacy of SBOM as a tool, and to motivate agencies to take the practice seriously rather than dismiss SBOM as part of a compliance checklist or documentation exercise.

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,

A handwritten signature in black ink, appearing to read "S. B. Lipner". The signature is fluid and cursive, with a small horizontal line at the end.

Steven B. Lipner
Chair
Information Security and Privacy Advisory Board

CC: The Honorable Alejandro Mayorkas, Secretary United States Department of Homeland Security, and
Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (CISA),
Department of Homeland Security