**U.S. Department of Homeland Security**
Cybersecurity & Infrastructure Security Agency
*Office of the Director*
Washington, DC 20528

July 25, 2023

Mr. Steven B. Lipner
Chair
Information Security and Privacy Advisory Board
c/o Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Dear Mr. Lipner:

Thank you for your May 15, 2023 letter to Secretary Mayorkas regarding Software Bill of Materials (SBOM) initiatives for Federal Agencies. I am responding on behalf of Department.

The Cybersecurity and Infrastructure Security Agency (CISA) is excited to partner with agencies across the U.S. Government on how best to turn SBOM data into usable information and use that information to drive actions to better defend our Departments and Agencies.

The National Institute of Standards and Technology (NIST) has been a strong partner in this effort, from NIST's work on SP 800-161 and SP 800-218 to the prominence of SBOM in joint discussions and public activities such as the Software and Supply Chain Assurance Forum. We have also briefed NIST's Information Security and Privacy Advisory Board several times, resulting in numerous substantive conversations with your members. We welcome further close collaboration.

While we wish to advance government use of SBOM, we are proceeding with appropriate prudence in advancing government-built solutions, as innovation may come more rapidly and effectively from experienced security vendors and a fast-growing number of startups. In working with the existing security tool marketplace, we believe that SBOM data can be a logical supplement to existing services and have heard from multiple vendors about upcoming plans for integration. In addition, we agree that rigorous metrics will be necessary to assess and validate the value of SBOMs in advancing defined cybersecurity outcomes, such as faster time to identify and remediate vulnerabilities – recognizing that prior events like our response to the "Log4Shell" vulnerability demonstrated challenges posed by the absence of SBOMs. As we expand adoption of SBOMs across products and agencies, we will simultaneously define and validate these types of outcome metrics.

As far as our ongoing work, the following activities will continue to provide additional opportunities for collaboration and feedback:

- As directed by the Office of Management and Budget (OMB) Memo 22-18, CISA is developing a "government-wide repository for software attestations and artifacts" in coordination with OMB and the General Services Administration which will accommodate SBOMs. A Request for Comment is currently open on this subject, with comments closing June 26, 2023.[1]

- CISA is planning to integrate SBOM data into our Continuous Diagnostics and Mitigation program to integrate asset inventory, supply chain, and SBOM data, enabling more effective management of and response to software security issues.
- CISA is working with NIST and the Office of the National Cyber Director to understand and enable more effective management of specific risks affecting open-source software, including as related to development and use of SBOMs, to the U.S. Government and critical infrastructure entities.

We welcome an opportunity to further discuss this topic with you or the broader ISPAB. Should you be interested in scheduling a meeting, please do not hesitate to contact me.

Sincerely,

Jen Easterly
Director

[1] Federal Register :: Agency Information Collection Activities: Request for Comment on Secure Software Development Attestation Common Form.