From: Nikhil Gupta
To: Friedman, Allan; Nikhil Gupta
Subject: ArmorCode Comment Letter, NTIA-2021-0001, SBOM Elements and Considerations
Date: Thursday, June 17, 2021 4:55:14 PM

Via Electronic Delivery: afriedman@ntia.gov

June 17, 2021

Allan Friedman
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

> **Re:** The Executive Order on Improving the Nation's Cybersecurity directing the Department of Commerce, in coordination with the National Telecommunications and Information Administration, to publish the minimum elements for a Software Bill of Materials
>
> **Focus:** "SBOM creation and use touches on a number of related areas in IT management, cybersecurity, and public policy" addressing the issue mentioned in "b. Software-as-a-Service and online services"

Dear Mr. Friedman,

Thank you for the opportunity to comment on the Software Bill of Materials (SBOM).

The Software-as-a-Service (SaaS) model of delivering applications has numerous advantages for both developers & consumers. The developers do not have to worry about the infrastructure resources by leveraging the cloud. The customers have access to the application from anywhere in the public domain without the need to go through Virtual Private Networks and Firewalls.

This model significantly increases the need of having more secure software because of ease of access to the applications from anywhere. It is critical to track the third-party components along with open source components to ensure that the company is addressing all the vulnerabilities and keeping the licenses for the third-party components up to date.

For SaaS vendors, it should not be mandated to publicly disclose the product SBOM as that may open the potential for attacks. Whereas current and potentially prospective customers should be able to follow

a predefined procedure, set by the SaaS vendor, to submit a request for SBOM information. The request would be evaluated on a case by case basis and the SBOM shared within 60 to 90 days.

In summary, in the SaaS model, we believe that the vendor should maintain SBOM internally which it can use for software security governance that benefits the end customer with the ability to know the components of the SaaS software.

Sincerely,

Nikhil Gupta,
CEO
ArmorCode Inc.
Email: ng@armorcode.io
Phone: +1 650-248-8585