SAFECode Comments on Software Bill of Materials Elements and Considerations

Response to National Telecommunications and Information Administration
Docket No. 210527-0117, RIN 9660-XC051

SAFECode is pleased to submit our comments in response to the NTIA's request for public comment on Software Bill of Materials (SBOM), Elements and Considerations. SAFECode has participated in the NTIA's Software Component Transparency initiative since 2017 and is aware of the opportunities and issues raised about the Software Bill of Materials.

SAFECode is a nonprofit industry organization that provides a global industry forum where business leaders and technical experts come together to exchange insights and ideas on creating, improving, and promoting scalable and effective software security programs. We believe that secure software development can only be achieved with an organizational commitment to the execution of a holistic assurance process, and that sharing information on that process, as well as the practices it encompasses, is the most effective way for software providers to help customers and other stakeholders manage software security risk. For almost fifteen years, SAFECode has engaged with companies and governments worldwide to encourage the adoption of effective software security processes.

SAFECode considers Executive Order 14028 to be a major step in the U.S. Government's recognition of the challenges posed by software security and initiation of measures to meet those challenges. The Executive Order will encourage software developers to adopt secure development processes of the sort that SAFECode has advocated since its founding in the mid-2000s.

The Executive order defines an SBOM as "a formal record containing the details and supply chain relationships of various components used in building software." Section 4 of the Executive Order requires that NIST publish guidance regarding "providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website" and that NTIA "publish minimum elements for an SBOM."

SAFECode strongly believes that software developers should have an SBOM for any product they sell. SAFECode has asserted this position for many years and most recently provided background and details in our 2019 paper "Managing Security Risks Inherent in the Use of Third-Party Components." Without an authoritative inventory of both open source and commercial third-party components (an SBOM), it is effectively impossible for a developer to assure the security of the software being delivered to customers.

As a practical matter, the use case for an SBOM relies on the actions of the software developer. The developer must monitor the quality and vulnerability status of third-party components, assess the impact of any vulnerabilities on the software in which they are embedded, and take appropriate action in response. The appropriate action may range from updating, replacing, or removing a component to changing configuration options or API calls to the component to determining that the vulnerability or issue does not affect the product. If necessary, the developer should provide customers with an update to the product and/or an advisory that identifies protective configuration changes or other mitigations.

The key point about application of the SBOM is that using the SBOM effectively requires analysis and evaluation by the developer. Even customers who have access to the SBOM are unlikely to have the in-depth knowledge of the embedding software to determine what action is appropriate to remediate or mitigate the effects of a vulnerability in a component. For developer-provided services or backend components, there is no effective action that the customers can take; they must rely on the developer.

Given this dependence on the developer, it is important to recognize that the value of an SBOM to software customers is limited to giving them confidence that the developer actually maintains an SBOM and is capable of following a process for promptly mitigating vulnerabilities in components upon discovery. The primary consumer of the SBOM is the software developer. Thus, there is little or no demonstrated value to standardized SBOM formats such as those listed in the request for comment. The SBOM content listed in the request for comment is sufficient for the purposes that an SBOM can serve – no expansion or elaboration is necessary.

In some cases, product developers may embed proprietary components whose inclusion is subject to a confidentiality agreement between component provider and product developer. Under those circumstances, the developer may be contractually prevented from disclosing the full product SBOM or may only be able to provide an SBOM under a nondisclosure agreement with the customer. Any guidance issued under the Executive Order should recognize and accommodate those limitations.

Much of the text in the NTIA request for comments describes benefits from an SBOM that are highly speculative. It is important that no guidance or requirements about SBOM be issued under the Executive Order until there are clear and complete demonstrations at scale that the putative benefits are in fact realizable.

SAFECode is happy to have provided these comments on the NTIA request for comment. Please feel free to contact Steven B. Lipner, Executive Director, SAFECode (lipner@safecode.org) if you have any questions.