aws

Amazon Web Services, Inc. ▪ 410 Terry Avenue N. ▪ Seattle, WA 98109

June 17, 2021

Ms. Evelyn Remaley
Acting Administrator
National Telecommunications and Information Administration (NTIA)
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

RE: AWS Comments on Software Bill of Materials Elements and Considerations (NTIA-2021-0001)

Dear Acting Administrator Remaley,

Amazon Web Services (AWS) appreciates the opportunity to submit the following comments to NTIA in response to the Software Bill of Materials (SBOM) Request For Comments (RFC). Security is our top priority, and we look forward to working closely with the United States (U.S.) Government to strengthen the security of its IT systems, as well as those of all our other customers. We believe it is important that all information technology providers utilize secure software development practices, and fully support the Government's efforts to improve evaluation and reporting on software provenance.

AWS appreciates the work of NTIA in development of the SBOM proposal. That said, while the NTIA SBOM approach may make sense for packaged software products, we do not believe it makes sense for cloud services (IaaS, PaaS, SaaS) as it will not support the government's cybersecurity objectives. Good software engineering practices play a key role in cloud service delivery; however, they are only one of many important elements that together determine the overall security of the service as provided. The security of cloud services should be assessed holistically in a manner that takes into account their full development and operational lifecycle.

We believe that any new work in assessing software provenance for cloud services would be better addressed in FedRAMP, the Federal Government's existing program for assessing the overall security of cloud services. FedRAMP already provides a well-known, widely-adopted, standardized approach to assess the security of cloud services and related products. FedRAMP is based on NIST's Special Publication 800-53 and associated standards. The FedRAMP office already leverages existing NIST recommendations as appropriate. The recent Executive Order (EO) on *Improving the Nation's Cybersecurity* specifically calls for the modernization of FedRAMP (EO, Section 3.f). Any additional requirements specific to software provenance and dependencies within cloud services should be addressed as part of that process. Introducing a separate approach and assessment requirement (such as SBOM) outside the much more holistic FedRAMP process will add unnecessary overhead for the government as well as cloud consumers and providers. It will cause duplication of work in FedRAMP, over-emphasize the issue of software provenance when considering the overall security posture of a service operated on behalf of customers by a service provider, and ultimately delay the adoption and use of cloud services. As noted multiple times in the EO, rapid migration to the cloud is a key aspect of the government's digital transformation and modernization initiatives and cybersecurity priorities.

After careful review of the questions in the RFC, we believe that more discussion is needed in order to identify the best way to achieve the requirements behind the SBOM proposal in the context of cloud services. We believe there are better ways to meet the requirements in that context than the mechanistic approach that seems to be envisioned. While we look forward to engaging in those discussions, hereafter we provide some high level feedback on the proposal from the perspective a major cloud service provider.

Service providers are accountable for the security of their service as a whole, not just the software elements. Cloud services are composed of dozens if not hundreds of microservices. These microservices are constantly undergoing rapid change, with new deployments often happening multiple times per day. Development/ operations teams that own individual constituent microservices must track their dependency chains for many reasons, including security-related issues, and address those appropriately. From an assessment perspective, the U.S. Government can require sound practices in software provenance and dependency management as part of FedRAMP, taking into account unique properties and benefits of agile, secure dev/ops engineering practices. Software vulnerability management is already in scope for NIST SP 800-53, verified through the audit process in FedRAMP. In the commercial sector, software vulnerability and provenance requirements are also audited through independent audit programs such as SSAE-18 SOC2, a time-tested model. These approaches minimize broad distribution of specific information that would be helpful to malicious actors and yet provide consumers with trusted third-party attestations of effective controls and practices based on clear evidence.

Providing secure services to our customers is our top priority, and we will work together with the U.S. Government to make sure their systems that utilize our services are as secure as possible. We look forward to future engagement with NTIA, NIST, and the FedRAMP Office on this effort to ensure that this class of requirements best support the government's goals and objectives. We are committed to collaboration with the U.S. Government in its implementation of the EO on *Improving the Nation's Cybersecurity* and the many related efforts to strengthen the the security of the Federal Government's IT systems and protect the Nation.

Sincerely,

Mark Ryland

Mark Ryland
Director, Office of the CISO
Amazon Web Services