June 17, 2021

The Honorable Evelyn L. Remaley
Acting Administrator
National Telecommunications and Information Administration,
U.S. Department of Commerce
1401 Constitution Avenue NW,
Washington, DC 20230

RE: Notice and Request for Comments on Software Bill of Materials Elements and Considerations

Comments of Salesforce.com, Inc.

Salesforce.com, Inc. ("we," "us," or "Salesforce") welcomes the National Telecommunication and Information Administration's (NTIA) effort to enhance the United States' software supply chain security. Salesforce respectfully submits comments on the minimum elements for a Software Bill of Materials (SBOM).

About Salesforce

Salesforce is a global leader in cloud enterprise software for customer relationship management (CRM), providing software-as-a-service ("SaaS") and platform-as-a-service ("PaaS") offerings to businesses. Founded in 1999, Salesforce provides business-focused software to businesses, governments and other organizations around the world. We operate in the business-to-business (B2B) environment, and our customers represent companies of all sizes and across all sectors. Our business model is subscription-based, allowing for faster deployment of technologies and greater agility. We help our customers connect with their customers — or employees or citizens — in a whole new way using cloud, social and mobile technologies.

Salesforce is committed to a set of core values — trust, customer success, innovation, and equality. Since we were founded, we have pioneered the 1-1-1 philanthropic model and each year we commit to giving 1% of our employee time, 1% of our product and 1% of our resources back to communities around the world.

Salesforce & Cybersecurity

Our customers are businesses who want to build stronger relationships with their customers and other stakeholders. As a result, customers trust us with some of their most sensitive data, making the protection of that data fundamental to our ability to serve our customers. It is why we have implemented a comprehensive and transparent privacy and security program, which includes achieving the authority to operate certain services at the FedRAMP High Impact Level and DoD IL4, as well as obtaining key certifications such as ISO 27001/17/18.

Our engineers build defense-in-depth into all of our systems because we know that taking a risk-based approach is critical to maintaining world-class security. We have more than 1,200 security professionals and dozens of security tools, processes and approaches to prevent, detect and respond to any security

threat. We implement the U.S. National Institute of Standards and Technology (NIST) cybersecurity framework (CSF). This metrics-based framework enables Salesforce to measure every security effort and project by tying it back to the five pillars of NIST CSF (Identify, Protect, Detect, Respond, Recover). Our risk-management program maps our security initiatives to the risks that they are meant to address. Some of the key areas of the program include risk assessments and reporting, including the risks posed by third-party products (3PP), product infrastructure, and the data supply chain. We conduct an annual security risk assessment on security risk areas across the company.

We have customers from around the world spanning dozens of sectors and industry verticals. We work closely with them to ensure that our data protection programs meet their diverse business and regulatory needs and requirements. This breadth and depth of experience gives us unique insights into approaches to cybersecurity that work—and we in turn share that information with our customers large and small. Salesforce believes that supply chain resiliency is a top priority; as a result, we offer the following additional specific insights and recommendations:

Clarity on Intent

As a SaaS and PaaS provider, we help support our customers by being strategic advisors in their security needs. From this viewpoint, we see a range in attitudes and knowledge regarding cybersecurity. Salesforce supports the stated goal of securing the software supply chain. However, SBOMs are a relatively new tool and we urge the NTIA to create a voluntary consensus standard. International standards provide broadly reviewed, consensus-based information and guidance for establishing and administering effective security methodologies, and facilitate common approaches to common challenges, thus enabling collaboration and interoperability.

SBOMs in their current form are merely a collection of constituent applications and infrastructure software of the final product or experience. While an SBOM can be valuable in helping engineers and other stakeholders gain an understanding of the software, it is only part of the information needed to determine the potential impact of any given vulnerability. Without clear understanding of how these software components interact, the true impact of specific vulnerabilities cannot be assessed. A cursory reading of the SBOM, its components and associated vulnerabilities might lead to misinterpretations and wrong conclusions if the connections between the SBOM components are misunderstood. It is important to understand that SBOMs will not be a silver bullet in helping with vulnerability management.

As a cloud company, our offerings change as we push updates to all of our customers. Therefore, we urge NTIA to consider a more flexible approach to the creation and maintenance of SBOMs that take into account the rapid innovation that can happen in companies providing cloud offerings. Finally, a further consideration for NTIA should be the scope and envisaged use cases for the SBOM. We encourage NTIA to provide clarity on the type of software that the SBOM should target as the inclusion of infrastructure components in the SBOM would be a considerable effort.

Security Concerns

Although an SBOM in and of itself does not include all the needed information to gain access to a SaaS, PaaS, or on-prem software deployment, listing out the set of software assets enables attackers to be able to easily cross reference publicly known vulnerabilities. Attackers can then focus on those vulnerabilities and exploit them to gain access. While vulnerabilities will be solved by patching, it is an acknowledged fact that there is a temporal gap between the existence, discovery and patching of a vulnerability. Therefore, as it relates to SBOMs, there must be the understanding that any additional information indicating a vulnerability, could be actionable. Salesforce would also note that the risk is especially increased for SaaS companies which provide a multi-tenant offering, for whom sharing of a single,

uniform SBOM would create risk for all customers who use the multi-tenant offering. A client (or adversary leveraging client access) can use legitimate access to the SBOM on behalf of its usage of the platform, to gain information that can be used to attack the SaaS provider and impact the other customers. Overall, SBOM could serve as an attack "blueprint" and public disclosure should, generally, be avoided.

In addition to the security concerns, public disclosure of SBOM could pose a risk to market dynamics. While the SBOM alone does not provide highly sensitive trade secrets like source code, it could still include other proprietary information such as the particular blend of software providers, vendors, and partners used to produce a given offering, which would constitute valuable intellectual property and proprietary information. Such information could expose market dynamics or be used by competitors to capitalize on opportunities of which they would be otherwise unaware. Most companies would typically only provide such information to a government customer under a promise of confidentiality, such that this information would be protected against disclosure by Exemption 4 to the Freedom of Information Act (FOIA), 5 U.S.C. 552.

Back-End Technology and Architecture

Given the sensitive nature of the SBOM, we would recommend that the NTIA consider more fully articulating the actual architecture and technology that will be used to organize and maintain the SBOMs.

While SBOMs can be a great tool, Salesforce cautions the aggregation of such data in one place, as it could be the target for bad-actors. Salesforce recommends that NTIA consider providing companies with guidance on building either complete or partial SBOMs to be available at the request of U.S. Government customers upon request.

In the document, NTIA said, "SBOMS should be available in a timely fashion and have proper access permission and roles in place[,]" this does not provide the level of security commensurate with the level of sensitivity included in SBOMs. Salesforce encourages NTIA to provide specific technical details regarding the types of data that they view as being critical. In addition, we recommend that SBOMs used for U.S. Government customers be treated as sensitive and proprietary, and marked as such, viewable only by U.S. government personnel with a need to know, and with appropriate exemptions from FOIA disclosure and from disclosure to other companies. Details on these questions will help drive clarity regarding the appropriate technical measures to take regarding the means of storage, access, and governance including the need for anonymization or tokens.

Conclusion

As a company, Salesforce is proud of our collaboration in the industry to invest in the necessary tools, training and support for everyone we work with and everyone who works for us. For this reason, we truly believe in the urgent need to continue to work toward a response to address systemic cybersecurity challenges and improve digital trust, to defend innovation and protect institutions, businesses, and individuals. We are proud to be a founding member of the Centre for Cybersecurity — established by the World Economic Forum.

Salesforce looks forward to working with NTIA and other agencies in the Federal Government to enact collaborative cybersecurity rules that enhance the United States' resiliency against cyber threats.

Respectfully submitted,
Jim Alkove
Chief Trust Officer