June 17, 2021

Ms. Evelyn Remaley
Acting NTIA Administrator
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

Dear Acting NTIA Administrator Remaley:

The Internet Association (IA) is pleased to share some views on behalf of our members regarding the Request for Comment (RFC) on Software Bill of Materials (SBOM) Elements and Considerations. IA is eager to support the implementation of the Executive Order (EO) on Improving the Nation's Cybersecurity and appreciates the opportunity to provide input on the minimum elements for an SBOM, and what other factors should be considered in the request, production, distribution, and consumption of SBOMs.

IA represents over 40 of the world's leading internet companies and supports policies that promote and enable internet innovation, including commercial cloud solutions. Our member companies are global leaders in the drive to develop lower cost, more secure, scalable, elastic, efficient, resilient, and innovative cloud services for customers in both the private and public sectors. IA members provide infrastructure (IaaS), platform (PaaS), and software as a service (SaaS) offerings across the globe. IA appreciates the continued engagement with industry and the opportunity to provide input on the policies considered by National Telecommunications and Information Administration (NTIA).

IA recognizes the considerable work that NTIA has undertaken since the inception of the initiative as well as the significant progress made to date. In particular, we recognize the commitment to consult with stakeholders throughout the development of the SBOM and are pleased that consultation is continuing as NTIA works to implement specific taskings directed in the EO. As we set out to respond to the RFC, we came to the conclusion that much of NTIA's work to date has been focused on a model of traditional software development and is most applicable to software running on customer premises or maintained by customers. The SBOM does not sufficiently account for some of the unique elements inherent in cloud services.

In our view, all "as a Service" delivery mechanisms present a different use case. The code base changes at a rapid pace. It is not unusual to update code used to provide the services in cloud environments multiple times a day. This reality would make an SBOM obsolete almost immediately and render it essentially meaningless for assessing risk. A customer would not benefit from a constantly changing document or manifest. We believe that a one size fits all approach has the potential to increase the risk to Federal networks by undermining the benefits of such services.

IA believes that NTIA should incorporate considerations unique to cloud services into the effort going forward. Accordingly, we recommend that NTIA, together with the National Institute of Standards and Technology (NIST), first work with FedRAMP to understand the current processes that are in place to mitigate risk in cloud offerings. FedRAMP provides an established and rigorous process and should be leveraged in considering any additional services assessment going forward. We also suggest that NTIA and NIST cloud consider the creation of a multi-stakeholder cloud working group, or some equivalent mechanism, comprised of government and industry subject matter experts to

jointly address related issues. This will ensure that future efforts around SBOM will be fit for purpose across multiple environments. As a first step towards this goal, IA respectfully requests a meeting with NTIA and NIST personnel as soon as possible to discuss our views as well as agree on how we can best support the effort going forward.

IA appreciates this opportunity to provide feedback on SBOM and its relationship to cloud, which represents a unique method of software deployment. We look forward to continuing to work with NTIA staff to implement this project such that the intended objectives are achieved.