Telecommunications Industry Association
1310 North Courthouse Road, Suite 890
Arlington, VA 22201 | www.tiaonline.org

SOFTWARE BILL OF MATERIALS ELEMENTS AND CONSIDERATIONS

A NOTICE BY THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
NTIA-2021-0001
June 17, 2021

REPONSE OF TIA:

The National Telecommunications and Information Administration (NTIA) recently issued a request for comment on Software Bill of Material (SBOM) Elements and Considerations[1]. Specifically, NTIA requests comments on the minimum elements of an SBOM across three areas: data fields, operational considerations and support for automation.

As NTIA considers SBOM elements, it is important that the agency makes use of work that industry has already begun in this area. The Telecommunications Industry Association (TIA) and its members believe utilizing SBOM will play a critical role in information and communication technology (ICT) security, and as an industry have been working for over a year and half on a process-based standard to help secure the ICT supply chain and address these concerns. The standard is based on ISO 9001 and TL 9000, the only process-based standard focused on communications service. Supply Chain Security (SCS) 9001 will be released by the end of 2021. SCS 9001[2] not only addresses the security of the ICT supply chain but also covers security of the software development process.

One of the more critical, and relevant to NTIA's request, subcommittees in the SCS 9001 working group is Software and Hardware Identification and Traceability. In order to assure software identification and traceability, the subcommittee is recommending that an organization create a process for a secure chain of custody that will implement methods to record system and component origin, along with the history of, changes to, and recording of who made changes. It also recommends an SBOM be created for all software, firmware and

[1] NTIA Request for Comments on Software Bill of Material Elements and Considerations, https://www.ntia.doc.gov/federal-register-notice/2021/notice-rfc-software-bill-materials-elements-considerations

[2] SCS 9001: The First ICT-Specific Standard for Global Supply Chain Security, https://mk0tiaonlinedevs02ww.kinstacdn.com/wp-content/uploads/2021/03/TIA-Supply-Chain-Security-PDF.pdf

supporting logic used in the creation of product and service elements. The combination of these requirements and methods will assure that the software component can be trusted.

Importantly, the SBOM recommendation proposed by SCS 9001 does include all NTIA's baseline component information.[3] SCS 9001 does expand on some of NTIA's baseline component items, introducing a dependency relationship by requiring software relationships, *i.e*., what is included in or derived from, further increasing software transparency and security. It also recommends identifying open source and third-party content for hardware and software.

Operational considerations -- frequency, depth, and delivery -- continue to be an important factor in the development of SCS 9001. For example, provenance methods identified include a depth of attributes including build location, license information/restriction, component integrity and transmission security. Frequency and delivery processes also continue to be evaluated by the subcommittee.

With regard to automation, there is strong support within SCS 9001 for the automation of creating and distributing SBOMs. TIA will continue to work on addressing automation tools.

As mentioned above, TIA and our members believe that SBOM is an important element for securing the ICT supply chain. As such, TIA's SCS 9001 currently recommends the use of SBOM along with methods and processes for how it should be used. These recommendations are consistent with the work being done at the NTIA, and we would welcome the opportunity to work with NTIA as it engages with industry on this critical issue.

Melissa Newman
VP, Government Affairs
TIA

[3] Baseline SBOM Component Information – supplier name, component name, component version, cryptographic hash of the component, other unique identifier, dependency relationship, author of SBOM data