Before the
U.S. DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Software Bill of Materials	)	Docket No. 210527–0117
Elements and Considerations	)	RIN 0660–XC051
	)	

COMMENTS OF
USTELECOM—THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association ("USTelecom")[1] is pleased to comment on the development and utility of a Software Bill of Materials (SBOM) in the National Telecommunications and Information Administration (NTIA)'s proceeding on SBOM elements and considerations.[2] USTelecom strongly supports the goals of NTIA in promoting a process which has the potential to reduce cybersecurity risks, enable better software security, and increase trust in digital infrastructure. In appropriate use cases, increased transparency in cybersecurity processes has the potential to remove barriers which limit the widespread sharing of information of risks and threats.

NTIA has done an admirable job of shepherding the SBOM initiative within the federal government and identifying the real security benefits in their appropriate contexts and use cases. As a broader set of government partners engage in this conversation, it is important to maintain the understanding that SBOM is not a capstone on software assurance, but instead one

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives—all providing advanced communications services to both urban and rural markets.

[2] National Telecommunications and Information Administration, U.S. Department of Commerce, Software Bill of Materials Elements and Considerations, Vol. 86, No. 104, Fed. Reg. 29568, (2021).

component of a holistic national strategy. Certain high-profile attacks against critical infrastructure, such as the cyberattack against SolarWinds, would not have been prevented by SBOM deployment. Thus, legislative solutions aimed at addressing attacks of that nature should not mandate the use of SBOM.

We offer the following insights based on consultations with our members in the telecommunications industry, with the goal of highlighting the connection between transparency in software processes and enhanced supply chain resilience.

I. USTelecom is Encouraged by NTIA's Multi-Stakeholder Approach to SBOM Development and Urges Federal Partners to Allow Enough Time for These Efforts to Reach Maturity.

USTelecom supports the goals of NTIA's SBOM initiative, which has the potential in a considerable variety of use cases to improve transparency and therefore cybersecurity within the software supply chain. Building resilient supply chains is crucial in a time of sophisticated malicious cyber campaigns that threaten American society. With this goal in mind, Executive Order 14028, "Improving the Nation's Cybersecurity"[3] tasks NTIA to define minimum elements for SBOM, an important step toward eventual deployment.

It is equally important, however, to ensure the final product is able to meet industry and government expectations, without giving rise to new problems. To that end, USTelecom encourages our partners at NTIA and across the federal government not to rush SBOM development, but rather allow enough time for this effort to reach maturity. In order to support the long-term capabilities of SBOMs, a large number of operational guidelines will need to be addressed. SBOM requirements should focus on a limited set of software applications, while

[3] *Improving the Nation's Cybersecurity,* 86 FR 26633, Executive Order 14028, at 26638 (2021).

allowing for increased individualization and company-specific specifications which will lead to greater widespread support and adoption of this process.

SBOM utility stems from the organization of software materials into a physical display of each aspect of the supply chain of a certain process. This data must be secured and uniquely identifiable to ensure the protection of sensitive data. The process of achieving appropriate levels of security requires further discussions and testing. We offer this as one example of the kinds of issues that remain to be addressed in order to make progress.

USTelecom is encouraged by NTIA's leadership and work so far, and we believe that if the agency continues to work on SBOM in collaboration with a broad set of participants in a multi-stakeholder process – allowing enough time for problems to be discovered and addressed thoroughly – this process is likely to result in a valuable tool for industry, which complements the other tools that industry uses to advance software supply chain security. Such outcome would naturally lead to voluntary adoption in appropriate use cases and preclude the need for unproductive procurement or regulatory requirements.

As NTIA considers the next phases of the SBOM initiative, such as its pilot program – which should reinforce the utility of voluntary and risk management based approaches to security – we encourage NTIA to continue considering input from the broad set of relevant stakeholders across the ICT sector. The ICT sector can contribute unique insights about how the creation and implementation of SBOMs affect diverse stakeholders, enabling NTIA to support individualized and rational goals for greater general utility of this new process.

USTelecom agrees strongly with NTIA's view that no one-size-fits-all approach should apply to providing transparency for software assurance. As such, USTelecom is encouraged by NTIA's statement regarding the individualized decision for publicity or privacy of SBOMs rather

than assuming a one-size-fits-all approach. As NTIA recognizes, "the act of making an SBOM is separate from sharing it with those who can use this data constructively. The author may advertise and share the SBOM at their discretion. In the case of publicly available open source software, it makes sense to make the SBOM public. In other cases, sector specific regulations or legal requirements may require more or less access to the SBOM."[4] These issues require adequate consideration from both the public and private sectors, as we continue working together towards shared security goals.

II. USTelecom Recommends NTIA Take a Holistic View of the SBOM Ecosystem to Ensure its Integrity.

It is already a recognized industry best practice for the software supplier to maintain an internal SBOM. Unique risks enter the picture, however, when exploitable information is shared externally. As NTIA works towards enhancing cybersecurity through SBOMs, it is crucial to consider how the information in SBOMs could be misused by malicious actors and what steps can be taken to ensure the security of the SBOMs themselves.

When externally sharing the sensitive information in the SBOM, a secure process must be built upon a foundation of confidentiality, authentication, integrity, and non-repudiation. Consideration needs to be made for processes that ensure secure transfer, receipt, storage, and access to the SBOM in-transit, at-rest, and in-use. The SBOM controller must provide controlled authorization to have privileged, secure access. It is recommended that these processes are contractual terms, while development of standards that could be referenced in the contract would enhance the processes.

[4] National Telecommunications and Information Administration, Draft for NTIA SBOM Multistakeholder Review at 7 (2021), https://www.ntia.gov/files/ntia/publications/ntia_sbom_faq_july9.pdf.

III. USTelecom Recommends NTIA Enable an SBOM Process Between Two Trusted Parties (Vendor and Customer).

Potential business and security issues for the network software vendor and operator would result from public disclosure of the SBOM. Public disclosure of the SBOM increases cybersecurity risk as it can be exploited by adversaries or cyber-criminals. Public disclosure can also compromise a vendor's business by allowing competitors, including those in adversarial nations, to gain knowledge about the use of proprietary, commercial third-party, and FOSS to reverse-engineer the application software. The SBOM for a network function should be provided to the network operator under contractual agreement subject to confidentiality provisions and with controlled distribution, without public disclosure.

IV. USTelecom Recommends NTIA Limit the Scope of SBOM to IT applications, excluding network, hosting, and cloud services.

The network, hosting, or cloud operator providing services should be responsible for collecting and using SBOMs from its vendors, provided under contractual terms, with the exception of the executable software components of these technologies.

V. USTelecom Recommends NTIA Implement Operational Elements that Provide Transparency and Efficiencies for Both the Generating and Storing Parties.

SBOM should be included in the software package at delivery. Access to the SBOM should be limited to a need-to-know basis and roles should be specified in the contract. Minimum fields in the SBOM for software transparency should be Component Name, Supplier Name, Version of the software component, and Origin (could be different than Supplier Name). Third-parties in receipt of SBOM must securely store the SBOM with modern ciphers for confidentiality and

integrity protection. SBOM should not be publicly disclosed. It is recommended that these processes are contractual terms, while development of standards that could be referenced in the contract would enhance the processes.

VI. USTelecom Recommends NTIA Continue Working with Industry on Numerous SBOM Operational Challenges.

As part of USTelecom members' ongoing commitments to software assurance and working in partnership with NTIA and other U.S. government partners, our members have identified a numbers of challenges that need to be addressed before operationalizing SBOM. The issues raised in this section are not exhaustive and should be viewed as part of a larger dialogue:

- To begin with, Executive Order 14028 defines an SBOM as "a formal record containing the details and supply chain relationships of various components used in building software"[5]. This definition could pose challenges or create confusion if applicable to legal contracts. For instance, in the case of open source software, authorship would be challenging to establish as part of a baseline component. Oftentimes, the author of open source software utilizes a pseudonym. In the case of open source, we recommend tracking the name (including the version number), URL of the open source, and identification of the open source license. For open source codes that require attribution, the SBOM should also include the proprietary/copyright notice for the open source code, and a copy of the open source license.
- Some tools for operationalizing SBOM do not presently exist or lack sophistication. Notably, the tools necessary for post-analysis of an SBOM (e.g., common exposure tools)

[5] *Improving the Nation's Cybersecurity* at 26646.

do not yet exist. The " ingredients" of software components are typically selected and architected into the software package during the software architecture/integration phase of the SW development Life cycle. Depending on the software development methodologies (e.g. Waterfall vs DevSecOps CI/CD) the release pipeline will vary (e.g. under SAFe, release units are delivered by sprint cycle, package is deployed rapidly and changes may be frequent to the process). The SBOM artifacts need to take into consideration the delivery, distribution and frequency under these continuous delivery environments.

USTelecom offers these additional recommendations in order to maximize the utility of NTIA's efforts related to SBOM:

- Include guidelines for length of time to retain SBOM.
- Identification of the proprietary of software code should be limited to the name and version number of the code, and should not include any information that could be used to deduce the source code.
- Include component license information and a time stamp. The time stamp is important because an SBOM is a snapshot in time.
- For open source packages, consider whether a list of contributors and country of origin may be useful. Country of original may only be obtainable for code produced by open source communities such as those managed by the Linux Foundation where contributors are registered.
- Include a runtime comparison of the SBOM to what is delivered, or a framework by which to abide.

- Do not include vulnerabilities in SBOM as vulnerabilities change regularly. Nonetheless, if the SBOM includes vulnerability data, then the source of the vulnerability data and the date the SBOM was created must be included in the SBOM.
- Software composition analysis software should have the ability to consume an SBOM and compare it to a vulnerability database and provide a date of the most recent update of the vulnerability database.
- For known vulnerabilities, an indicator should be included in the SBOM data model, along with a pointer to the test or analysis proving that the vulnerability is ineffective or to mitigating controls.
- The names of the component packages bundled in object code are usually different than the actual names collected from the package managers in the source code. It may be useful to have an optional alias field to show the relationship between the names.
- Use digital signing authorities with public X.509 certificates to authenticate the source. For example, the Linux Foundation supports trusted signing for all projects under their umbrella.
- In order to gain consistency and accuracy on the source data used to generate SBOM, topics such as when/where/by who SBOM should be generated. This feature will be more impactful if it is baked in as part of the software development process, specifically the architecture/design and release management phase. The disclosure, delivery, distribution and management of SBOM will need an industry-wide collaboration and adaptation effort. Participation from industry best practice organizations (e.g., ITIL – formerly "Information Technology Infrastructure Library") and standard bodies (e.g., ISO – the International Organization for Standardization), will be helpful.

- As consumers on the software supply chain, some common tools and methodologies should be evaluated/made available to help unpack, identify, analyze, test and validate a software application package and all its dependencies and components. A standardized and unifying way to structure and evaluate the breakdown of the software ingredients.
- To effectively manage risk from SBOM, vulnerabilities and threats need to be assessed and validated in a timely manner. SBOM can benefit from a life cycle approach to manage risks, integrating into NIST Cybersecurity Framework that include key categories such as Identify, Protect, Detect, Respond, Recover.
- There need to be use cases focused on IoT, IIoT and SCADA type software. The architecture composition and software components incorporated into the embedded systems such as GPS devices, industry machines/controller/ gateway, field devices, supervisory units, PLC, robotic systems, vision/camera systems, etc. often contain legacy code, third party code and binary reuse.

VII. Conclusion

USTelecom appreciates this opportunity to provide insights regarding SBOM elements and considerations and urges our partners at NTIA, as well as the broader set of government stakeholders evaluating these issues, to adopt the approaches described in these comments.

Respectfully submitted,

USTELECOM – THE BROADBAND ASSOCIATION

By: */s/ Paul Eisler*
Paul Eisler
Grace Motta

601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001
(202) 326-7300

June 17, 2021