MITA®
MEDICAL IMAGING
& TECHNOLOGY ALLIANCE
A DIVISION OF NEMA®

1300 North 17th Street ▪ Suite 900
Arlington, Virginia 22209
Tel: 703.841.3200
Fax: 703.841.3392
www.medicalimaging.org

6/17/2021

Ms. Evelyn L. Remaley
Acting NTIA Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

RE: Federal Register Docket No. 210527-0117 (NTIA-2021-0001)

Dear Ms. Remaley,

As the leading trade association representing the manufacturers of medical imaging equipment, radiopharmaceuticals, contrast media, and focused ultrasound therapeutic devices, the Medical Imaging & Technology Alliance (MITA) applauds the National Telecommunications and Information Administration in its continued work to enhance software supply chain security and submits these comments in support of that goal.

The elements and factors outlined within NTIA-2021-0001 provide a strong foundation for the initial adoption of the Software Bill of Materials (SBOM) as another tool to improve cyber resilience. However, certain details contained and omitted from the text do require additional clarification. A more complete discourse to describe the intersection between SBOM and other security tools would also be welcome. The comments below aim to identify these areas of potential confusion and, where appropriate, propose solutions for NTIA consideration.

Minimum Elements for an SBOM
The document's stated purpose is to publish "minimum elements for an SBOM". However, it is unclear whether the published elements would constitute a requirement or a recommendation. This issue intensifies during the discussion of data field expansion. We recommend that NTIA clearly indicate, in its final publication, whether the elements are required or recommended. For purposes within this letter, MITA assumes the proposed minimum elements will be required.

Ultimately, a precise standard for SBOM should be identified, with clear definition of the minimum requirements for content, before SBOM becomes mandatory. Until the software industry aligns on a standard, it does not make sense to mandate suppliers to provide information if they might incur significant costs in retooling to later changes.

Data Fields
Clarity of the labels proposed for data fields is critical to the ultimate success of the SBOM. Unfortunately, the labels provided (supplier name, component name, version of the component, cryptographic hash of the component, any other unique identifier, dependency relationship, and author of the SBOM data) are not all easily understood.

"Supplier Name" is too ambiguous and could lead to misidentification. We understand the label to mean the software or component supplier, such as an original developer, but could easily be understood as the entity selling the software or component, among other interpretations.

"Author name" is similar. Does it refer to the document's author? The author of the item? Does the author change when an SBOM changes hands and is expanded as it travels the supply chain? If the intent is to identify the original information source for the component, we propose changing the field label to "Component Information Source" or similar.

"Any other unique identifier" does not belong in a minimum set of required fields, as the word "minimum" suggests additional fields could be added at the discretion of the author. Inclusion would work against the standardization this effort aims to accomplish by allowing an unlimited number of variations for one field.

"Cryptographic hash of the component" is unclear. The following questions are unresolved:

1. Does the consumer of the SBOM use the hash to uniquely identify the component or to confirm its integrity?
2. Are all files to be included as shipped?
3. Is it a hash of the installation package or files after installation?
4. What about systems that are highly customized, perhaps not until deployment time?
5. Is it for executable files only, or does it include all files installed and subsequently configured for the component?

Absent satisfactory answers to these questions, we recommend cryptographic hash be omitted from the set of minimum elements.

"Dependency relationship" suggests a tree structure which identifies subcomponents and subcomponents of subcomponents. However, the value provided by such a structure is questionable for all use cases. The value comes from identifying the components regardless of dependency. We recommend this element be omitted from the minimum element list.

The data field expansion and "dependency relationship" example are also cause for confusion. Field expansion is outside the conceptual scope of minimum, and again muddies the case for standardization. The field dependency relationship would be of limited use if the same information type was not provided in every SBOM generated. The examples (reference standards, tools used, build process) would be better provided in separate, optional fields as determined by the SBOM supplier.

MITA recommends the NTIA adopt the following elements as the only required minimum element set: "Supplier Name", "Component Name", "Component Version", "Author Name" (or "Component Information Source"). The remaining elements identified in this RFI ("Any other unique identifier", "Cryptographic hash of the component", and "Dependency relationship") may be better suited for optional, use case specific supplements.

Operational Considerations

This section asserts that SBOM is more than a set of data fields. While the intent may be obvious to those well versed in software transparency, the statement itself is inaccurate. The SBOM is, ultimately, a security document. This should be corrected to reflect that SBOM creation and use requires certain operational considerations—which could be achieved by removing the indicated statement, "SBOM is more than a set of data fields".

Request for Comment – Questions

1. Are the elements described above, including data fields, operational considerations, and support for automation, sufficient? What other elements should be considered and why?

The seven data fields proposed go beyond an appropriate minimum required element set and should be reduced to the following: "Supplier Name", "Component Name", "Component Version", "Author Name" (or "Component Information Source"). Removing "Any other unique identifier", "Cryptographic hash of the component", and "Dependency relationship" would promote better standardization and achieve this effort's indicated goals.

…

3. SBOM creation and use touches on a number of related areas in IT management, cybersecurity, and public policy. We seek comment on how these issues described below should be considered in defining SBOM elements today and in the future.

a. Software Identity: There is no single namespace to easily identify and name every software component. The challenge is not the lack of standards, but multiple standards and practices in different communities.

Partial standardization of software naming practices by identifying acceptable standards (e.g., CPE)—even as examples—could help reduce variability in the short term. As more organizations produce their own SBOMs, the original component manufacturer should exert more control over their own component names.

In addition, this software identity problem would reoccur with the cryptographic hash field. Similar issues—different hashing protocols, multiple standards—challenge standardization.

b. Software-as-a-Service and online services: While current, cloud-based software has the advantage of more modern tool chains, the use cases for SBOM may be different for software that is not running on customer premises or maintained by the customer.

SBOM benefits both suppliers and consumers. Cloud software providers should still be expected to maintain and provide information about their platforms, the software they run, and the plugins they use. Cloud software, then, becomes another example of SBOM "depth" as contemplated by NTIA.

c. Legacy and binary-only software: Older software often has greater risks, especially if it is not maintained. In some cases, the source may not even be obtainable, with only the object code available for SBOM generation.

If a source is unknown, that should be indicated in the source field as provided by the minimum elements. Similarly, if information is generated by a tool, then that tool should be identified as the source. The supplier may intentionally omit certain information (e.g., to protect intellectual property) or may be forced to do so—either

because the information is not provided by the component supplier or because the original source code is not available. Such instances should be explicitly indicated in the SBOM.

…

f. High assurance use cases: Some SBOM use cases require additional data about aspects of the software development and build environment, including those aspects that are enumerated in Executive Order 14028**.[**13**] How can SBOM data be integrated with this additional data in a modular fashion?**

Elements necessary to support specialized use cases, including industry specific use cases, may supplement the minimum elements. The SBOM provider should retain flexibility in which additional elements provide support for their specific use case scenarios since supplemental elements may only be of use to certain industries and suppliers. Supplements to address industry specific use cases should be developed with associations and interests that represent those industries.

g. Delivery. As noted above, multiple mechanisms exist to aid in SBOM discovery, as well as to enable access to SBOMs. Further mechanisms and standards may be needed, yet too many options may impose higher costs on either SBOM producers or consumers.

Delivery methods are best determined by market forces. Customers within different markets may have different requirements, which suppliers will be incentivized to respond to. Delivery requirements, especially those proposed for all markets, should be avoided.

h. Depth. As noted above, while ideal SBOMs have the complete graph of the assembled software, not every software producer will be able or ready to share the entire graph.

As noted in the comment in response to 3c, a supplier may intentionally omit certain information (e.g., to protect intellectual property) or may be forced to do so—either because the information is not provided by the component supplier or because the original source code is not available. Such instances should be explicitly indicated in the SBOM.

i. Vulnerabilities. Many of the use cases around SBOMs focus on known vulnerabilities. Some build on this by including vulnerability data in the SBOM itself. Others note that the existence and status of vulnerabilities can change over time, and there is no general guarantee or signal about whether the SBOM data is up-to-date relative to all relevant and applicable vulnerability data sources.

A public SBOM in not a standalone solution to manage risk and is intended to be used in conjunction with additional risk management. It supports those processes

alongside other security documentation, such as the healthcare sector's Manufacturer Disclosure Statement for Medical Device Security, and existing supplier and customer processes. This information should be well documented alongside any discussion or description of SBOM and its use.

As mentioned in response to part f, highly specialized use cases like vulnerability management may supplement the minimum elements. Although vulnerability management use cases may be more common than others, they are not universal, and we encourage any reference to fields which support use cases (e.g., VEX) be incorporated into a supplement or appendix distinct from the minimum elements.

Finally, Given the different timeframes that might exist between the generation of SBOMs and the surfacing of vulnerabilities, it would overly burden the SBOM to include vulnerability information directly within it.

We count on your attention to these comments. If you have any questions, please contact Zack Hornberger, Director of Cybersecurity & Informatics, at zhornberger@medicalimaging.org or 703-841-3285.

Sincerely,

Patrick Hope
Executive Director, MITA

MITA is the collective voice of manufacturers of medical imaging equipment, radiopharmaceuticals, contrast media, and focused ultrasound therapeutic devices. It represents companies whose sales comprise more than 90 percent of the global market for medical imaging innovations. These products include: magnetic resonance imaging (MRI), medical X-Ray equipment, computed tomography (CT) scanners, ultrasound, nuclear imaging, radiopharmaceuticals, and imaging information systems. MITA Member company technologies are an important part of our nation's healthcare infrastructure and are essential for the screening, diagnosis, staging, managing and effectively treating patients with cancer, heart disease, neurological degeneration, and numerous other medical conditions.