AdvaMed
Advanced Medical Technology Association

701 Pennsylvania Avenue, NW
Suite 800
Washington, D.C. 20004–2654
Tel: 202 783 8700
Fax: 202 783 8750
www.AdvaMed.org

June 17, 2021

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW, Room 4725
Washington, DC 20230

Re: Docket No. 210527-0117: Software Bill of Materials Elements and Considerations

To Whom It May Concern:

The Advanced Medical Technology Association ("AdvaMed") appreciates the opportunity to provide feedback on the National Telecommunications and Information Administration's ("NTIA") request for comments ("RFC") concerning Software Bill of Materials Elements and Considerations.[1] AdvaMed represents manufacturers of medical devices, digital health technologies, and diagnostic products that transform health care through earlier disease detection, less invasive procedures, and more effective treatment. Our members range from the smallest to the largest medical technology innovators and companies.

AdvaMed commends the work NTIA has conducted on software component transparency over the last several years.[2] We believe the multi-stakeholder effort, which brought together key stakeholders in the community—including medical device manufacturers and hospitals—serves as a strong foundation for the NTIA's current efforts to carry out the President's Executive Order on Improving the Nation's Cybersecurity ("EO").[3]

We recognize developing a one-size-fits-all approach to describing the elements and considerations for a software bill of material ("SBOM") can be difficult given the diverse nature of industry's that are impacted, both in general and directly through the EO. Nevertheless, we believe that, in general, the RFC takes an appropriate approach, and identifies the key elements and considerations for an SBOM. Our specific comments on and responses to the questions contained in the RFC can be found in the attached chart.

[1] *Available at* https://www.ntia.gov/federal-register-notice/2021/notice-rfc-software-bill-materials-elements-considerations.

[2] *See* https://www.ntia.doc.gov/SoftwareTransparency.

[3] *Available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

We thank you for your consideration of these comments. Please do not hesitate to contact me at zrothstein@advamed.org should you have any questions.

Respectfully submitted,

/s/

Zachary A. Rothstein, Esq.
Senior Vice President
Technology and Regulatory Affairs

Attachment

AdvaMed Comments

Software Bill of Materials Elements and Considerations

Question/Location	Comment/Proposed Change	Rationale
General comment	We recommend NTIA add a statement to ensure readers consider the information provided in the SBOM in the context of a broader cybersecurity protection strategy (*e.g.*, network security, physical security, and layered protection).	While the SBOM is a critical element of cyber security, it is only one aspect of a comprehensive cyber security strategy typically employed by organizations. If the SBOM is consumed without consideration for layered controls, inappropriate assumptions regarding risk may be made. Therefore, we recommend NTIA help educate the cybersecurity community to consider the SBOM in the appropriate context.
General Comment, Page 4	We recommend clarity of SBOM definitions. Various components concept should be clarified.	From technical perspective, components to build software can be a technology tools.
p. 5, Data fields	We recommend providing information on the expected depth of dependency relationships (*e.g.*, which relationships should be defined as a baseline?).	Dependency relationship could be at the package level or down to libraries. Complexity of this mapping could vary greatly.
p. 5, Data fields	We recommend clarifying that components include Off-the-Shelf, custom build, and open source software, including operating systems.	Adding this clarity will assist the utility of the SBOM.
p. 5, Data fields	Please describe the method to create a cryptographic hash for a highly complex component, such as an operating system.	The use of a hash is poorly defined. 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?

		If it is not possible to directly answer these questions, then cryptographic hash should not be identified in the set of minimum elements.
p. 6, Operational considerations	SBOMs should include version numbers	Each change to an SBOM should result in a new version identification so that component changes can be easily traced.
p. 8, Question 2	A challenging use-case has been determining whether a medical device contains components that are vulnerable to groups of vulnerabilities (*e.g.*, Urgent/11, Ripple20)	Our current process includes individually contacting suppliers and asking them to verify whether their components use any of the underlying systems affected by the vulnerabilities. It can be a slow process and makes it difficult for a device manufacturer to know if our products are exposed.
p. 8, Question 3.b	We believe the vendor/supplier of a SaaS should be responsible for maintaining the SBOM and identify, mitigate, and notify its customers in the case of an issue.	The vendor/supplier will have the most accurate and up to date information.
	Given that systems can rely on SaaS products maintained by a 3rd party, clarity is needed on whether SaaS SBOMs should be designed to be accurate at the time of viewing or accurate at the time of generation.	3rd-party managed systems such as SaaS products can be updated outside of product release cycles.
p. 10, Question 3.h	The issue of "depth" should be generalized to "completeness." An SBOM should have an indication where there is data missing and the reason for the gap (intentional/unknown).	As noted in the rationale to the comment on question 3.c, the lack of completeness may be either at the decision of the supplier or represent the inability of the supplier to fully specify all the components. In any case there should be explicit acknowledgement of component-level opacity in the SBOM.
General comment	A detailed standard for SBOM should be identified, with clear definition of the minimum requirements for content, before SBOM becomes mandatory.	Until the software-creating industry aligns has a specific standard or standards for SBOM, it does not make sense to mandate suppliers to provide information if they might incur significant costs in retooling to later changes. The government can take a more active role in defining a standard.
General comment	NTIA should clarify whether a human readable SBOM will also be expected.	We believe prior discussions within the NTIA multi-stakeholder effort debated this question.
General comment	NTIA should clarify whether an SBOM should include non-saleable web applications that work alongside of products.	There are often apps and other software that provide support functions, such as transferring

		data between products and/or customer support services.
General comment on the use of the term "component"	We recommend NTIA state that "components" are units of software and attributes are information about components, consistent with the report produced by the NTIA framing working group. *Available at* https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf.	The term component is defined in other regulatory contexts, so it is important for NTIA to be clear what the term refers to. For example, the U.S. Food and Drug Administration, which supports medical device manufacturers submitting an SBOM to the Agency, defines component at 21 C.F.R. § 820.3(c) as "any raw material, substance, piece, part, software, firmware, labeling, or assembly which is intended to be included as part of the finished, packaged, and labeled device."