SUBMITTED ELECTRONICALLY VIA REGULATIONS.GOV

June 17, 2021

**Subject: Software Bill of Materials Elements and Considerations**

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

To Whom It May Concern:

UL appreciates the opportunity to comment on the National Telecommunications and Information Administration's (NTIA) Notice and Request for Public Comment on Software Bill of Materials Minimum Elements to the President's Executive Order on Improving the Nation's Cybersecurity. UL supports NTIA seeking information to understand the industry's current practices to identify and mitigate cybersecurity vulnerabilities in the software ecosystem.

Since its inception in 1894, UL serves a mission of promoting safe living and working environments for people everywhere and fulfills a promise of facilitating the flow of goods across borders. Grounded in science and collaboration, UL's work empowers trust in pioneering technologies, from electricity to the internet. We help innovators create safer, more secure products and technologies to enable their safe adoption.

UL appreciates NTIA's several mentions of standards in the development of a Software Bill of Materials (SBOM) in the notice and request for comment. As a leading global standards development organization (SDO) and third-party certifier, UL is uniquely positioned to assist NTIA in its verification of minimum standards for Software Bill of Materials.

NTIA should have confidence in leveraging standards and frameworks developed by private standards development organizations (SDOs). Most SDOs are governed by principles of transparency, openness, impartiality, consensus, lack of dominance, due process, and benefit from the participation of affected stakeholders representing a wide variety of viewpoints and perspectives. SDOs play a significant role in international standards harmonization and development, helping to satisfy trade commitments, demonstrating leadership in the application of good regulatory practices, and setting standards that provide the basis for conformance required for market access for US products and services and the enablement of fair and reciprocal competition.

UL recommends that NTIA participate in and contribute to private sector-led standards development to inform the development of cyber-related standards. In addition, NTIA should consider the potential value-added role third-party conformity assessment bodies can play in providing independent verification of conformance to these standards and frameworks and cybersecurity efforts reported by organizations. In relying on private sector conformity assessment providers, regulators can reduce both implementation costs and compliance burdens.

Please find below UL's detailed responses to a subset of the questions posed in the Request for Information. As NTIA moves forward with its efforts to advance cybersecurity and minimum elements of a Software Bill of Materials, UL is eager to share our expertise with NTIA. If you have any questions regarding this submission or would like to discuss UL's recommendations further, please do not hesitate to contact Thomas Daley, UL Global Government Affairs, at thomas.daley@ul.com. Thank you for your attention to these comments.

Respectfully,

Derek Greenauer
Director, Global Government Affairs

______________________

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

One key idea, whether as part of an SBOM or adjacent to an SBOM, is that you can track and manage vulnerabilities using an SBOM. For that to be possible you need to be able to split a component into discrete parts for each of which you want to assign an origin and owner, and ideally this owner tracks vulnerabilities for that discrete part or it has vulnerabilities posted against it (for example, an open source library). Now if these discrete parts are for example including Windows 10, that could be granular enough since (ideally) MS tracks vulnerabilities for Windows 10 and all its dependencies. So, in the ideal case you could reference MS's info on vulnerabilities for Windows 10 version x,y,z and stop there. If these discrete parts are part of some IoT device or system e.g. with a few hundred open source libraries and programs where an owner is not actively managing information, you'd want to know the details of all the discrete software parts to be able to track this information down. In the latter case, therefore you'd want to be able to construct a tree or dependency graph based on a root component ending with components that have no further dependencies. With the current proposed SBOM data structure, without a more precise definition of dependencies, it's not clear how this can be done.

From an automation POV, key aspects to support would be automatic generation and machine-readability for SBOM repositories. E.g., for machine readability an SBOM can embed a unique SGUId (SBOM Graphical User Identifier) into each (functional) bit of compiled software [package, blob, program]. In the end, it should be possible to tie each bit of software to an SBOM so it can be determined if a) you are running this code; and b) are there any documented vulnerabilities of concern? A device can SHA2 any bit of code prior to executing and compare to the repository SGUId-SHA2 (which could be stored in flash for efficiency reasons).

**2. Are there additional use cases that can further inform the elements of SBOM?**

Given that one main use case for SBOMs is performing vulnerability management, some standardized method for referencing CVE info for both public and private software would be useful to be included (for example, a standard url for the manufacturer to implement to point to CVE data or to a public CVE tracker). I.e., ideally it should be possible to figure out from a dependency graph which software has publicly tracked CVE information that can be retrieved in an automated way, and which software is proprietary and requires manual investigation.

**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.**

Per the answers to questions 1. and 2., SBOM creation and management can touch on vulnerability management as an important use case.