LUTA SECURITY

June 17, 2021

Ms. Evelyn Remaley
Assistant Secretary of Commerce for Communications and Information
United States Department of Commerce
National Telecommunications and Information Administration
1401 Constitution Avenue NW, Washington, D.C., 20230

Submitted via email to SBOM_RFC@ntia.gov.

RE: Department of Commerce and National Telecommunications and Information Agency's "Software Bill of Materials Elements and Considerations" 86 Federal Register 104 (June 2, 2021) [Docket No. 210527-0117; RIN 0660-XC051]

Dear Acting Assistant Secretary Remaley,

Thank you for the opportunity to comment on these proposed elements for a Software Bill of Materials (SBOM). Luta Security is a security company that works with governments and complex organizations to transform the way these organizations use people, processes, and technology to create mature, robust, and sustainable vulnerability disclosure and bug bounty programs. We are pleased to provide comments on the Department of Commerce's and National Telecommunications and Information Administration's (NTIA) Docket No. 210527-0117 / NTIA-2021-0001.

Luta Security believes that the concept behind SBOM is laudable, though, in its current inception, its introduction may divert time and effort from other more immediately beneficial cybersecurity measures and initiatives, which in turn can cause more issues for national security than it solves.

As noted in several NTIA publications, the definition of an SBOM is still unclear:

> "A "Software Bill of Materials" (SBOM) is effectively a nested inventory, a list of ingredients that make up software components."[1]
>
> "Q: What is an SBOM?
> A: A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of various components used in building software."[2]

[1] https://www.ntia.gov/SBOM
[2] https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf

SBOM Case Study Flaws

As noted in the assertions from NTIA and the Multistakeholder working group's case studies and FAQs, there are several areas that are not consistently defined. The definition of SBOM itself is not defined yet, which is one of many concerns I have in the rapid implementation of SBOM as a new Federal requirement for software acquisition. This public comment period of 15 days to gather industry input also heavily relies on stakeholders who have the time and capacity for such a short turnaround, leaving out participation from smaller organizations that are likely to be negatively impacted by sudden new requirements.

The assertions made by the proponents of SBOM, including the case studies published by the NTIA working groups, do not contain any data proving their assertions. For example, the common assertion by SBOM proponents that SBOMs speed up delivery of fixes across an entire supply chain has not been adequately studied. To reach the desired outcomes of reduced time to fix across the software supply chain it requires well-equipped multiparty vulnerability coordination capabilities.

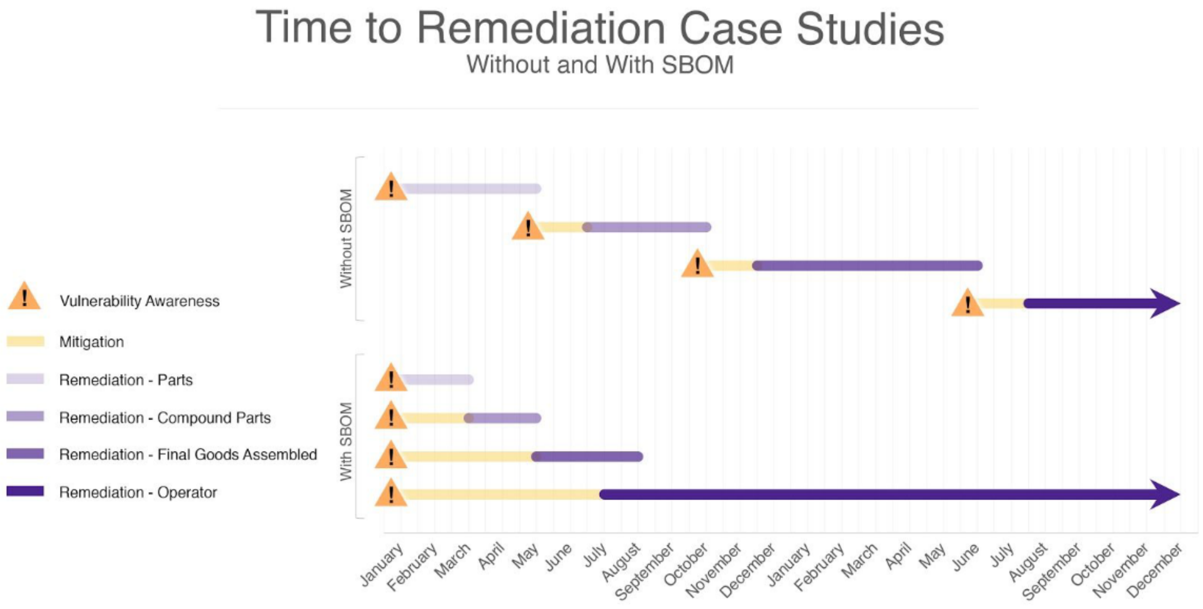

Figure 2: Time to Remediation Case Studies - With and Without SBOM

The graph's premise is not supported by data included or referenced in the report, nor does it represent real world multiparty vulnerability coordination.[3] In the above chart, the argument made is that with an SBOM, all pieces of the supply chain can work on fixes at once. This is a false correlation between speed of fixes and the presence of an SBOM.

[3] https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

While I agree that knowing which other security teams an organization needs to contact is essential, an SBOM alone gives you no advantage in trying to forge those team-to-team relationships ahead of a security incident that spans the supply chain.

In reality, if a component is vulnerable, regardless of an SBOM, the speed at which others in the supply chain can work on their fixes is determined by the presence and robustness of a multiparty vulnerability coordination capability – when the issue is privately disclosed to at least one member of the supply chain. Fixes across a supply chain can be sped up by building a Coordinated Vulnerability Disclosure (CVD) multiparty capability, which is a labor-intensive mechanism that is nontrivial to establish.

Without SBOMs, the graph illustrates that the supply chain vulnerability handling is serialized, with each member of the supply chain only beginning to work on their fixes after the previous supply chain member has completed their fix. The reality is different in most cases.

When a vulnerability in a component is publicly disclosed, either via explicit disclosure in an advisory or exploit, or via the release of a new version of an affected package in the supply chain, all other members of that supply chain would be able to work on their fixes at once.

The idea that fixes without SBOMs are universally delayed because the supply chain members are dependent on completion of one supply chain member at a time is not supported by data.

While the quote and note below point out the benefit of CVD in "enhancing" the effect of SBOM adoption, the reality is that multiparty vulnerability coordination is required to make use of SBOM in the first place. Despite the ISO standards and NTIA guidance on vulnerability disclosure, widespread industry and government adoption of these practices have not been broadly implemented. This is true of simple CVD programs, let alone CVD programs that are capable of performing multiparty vulnerability coordination. The United States government only started rolling out its own VDPs as of March 2021.

> "With the improvements brought about through the use of SBOMs, each link of the supply chain could become aware of new vulnerabilities at the same time. Workarounds and mitigations could be put into place immediately while long-term fixes are under development.
> NOTE: This opportunity is even further super-charged in combination with benefits of NTIA's other Coordinated Vulnerability Disclosure working groups where initial patches have been made available prior to any adversary awareness."[4]

The presence of an SBOM has no tangible or measurable effect supported by data in NTIA's own case studies, but the presence of a robust multiparty vulnerability coordination capability does affect the speed of comprehensive supply chain security.

[4] https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

These “case studies” are devoid of data for their stated assertions, and more importantly, leave out data on the people, process, and technology that is required to understand the true cost and mechanisms by which SBOMs can make a tangible speed difference.

While the concept of SBOMs is useful, it cannot be mistaken for a way to address software supply chain risk management on its own. There are unintended consequences of imposing an undefined, non-standardized, and unproven mechanism upon federal contractors. As we work to elevate the security of all members of the supply chain, SBOM production and consumption can be a potentially costly distraction from more directly useful activities.

We must ensure that we take the limitations of SBOM into consideration as we weigh the return on investment for all of the important cybersecurity initiatives in the Executive Order[5]. Under a global cyber workforce shortage, especially across the United States,[6] spinning up workers to meet these requirements will have an opportunity cost of forgoing other essential cyber resilience activities.

An ingredient list of software alone is not useful to determine risk quickly without additional analysis by skilled workers. Neither is the addition of vulnerability data, which would at a minimum include what known vulnerabilities affected each software ingredient. This is because from a technical standpoint, a bug in a software ingredient may not be exploitable in all products that contain that software ingredient. Exploitability would be determined in what code paths are taken via the product, and what other countermeasures may be in place in the overall product that obviate or mitigate the underlying software supply chain vulnerability.

There are no tools that can produce this enriched vulnerability data that includes vetting actual exploitability at scale. This ends up in the same resource crunch situation relying on skilled cybersecurity workers to make that final determination of risk and act upon it.

Data Fields

Much of the difficulty behind SBOM is that it does little to actually disclose potential vulnerabilities within a product’s software. We understand that by definition an SBOM does not include vulnerability information. That is why pushing for SBOMs is not immediately useful for increasing supply chain security.

For example, if a product uses software A, and known vulnerability X exists in software A, it does not immediately follow that vulnerability X *can* be exploited in the product. The product may have other countermeasures and security processes in place to prevent vulnerability X (whether directly or indirectly), or it may just be that the coding paths in the product coupled with the use of software A does not provide a real security risk. While all of the data fields that NTIA identify are important, they do not reveal the whole picture.

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

[6] https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

As noted in the Executive Order, it is important that the minimum elements for SBOMs need to be defined; however, the timeframe is incredibly short to create a standard. True case studies with data and cyber workforce requirements should be performed before mandating SBOMs. Not only would this assist in elucidating useful versus extraneous data to include — potentially lightening the workload, whether by individuals or automated systems, of creating SBOMs — but it would also provide further clarification as to *how* these data should be understood. As noted above, the same software in one product versus another does not necessarily create an equal vulnerability risk. Knowing, categorizing, and publishing the coding paths between different software in an SBOM, while work-intensive, would provide a much clearer picture of potential vulnerabilities.

Operational Considerations

Of course, the operational considerations that the NTIA identify could provide some clarity as to whether a "potential" vulnerability is actually a real vulnerability in a product. Knowing the dependency chain of a software (or even just acknowledging the "known unknowns") can provide cybersecurity specialists with the information to make rational analysis and judgements about the possible exploitability of the product. However, even if an SBOM *does* reveal useful information about likely exploitable vulnerabilities in software, it is another question entirely as to whether the workforce and resources exist to monitor and patch these vulnerabilities. Many in the cybersecurity industry are already aware of the current gap between cybersecurity roles and individuals to fill said roles. Large organizations may be able to effectively implement an SBOM, act on vulnerabilities, and disclose hacks, but smaller organizations with less resources may be hamstrung in attempting to publish or consume SBOMs and take all necessary steps after-the-fact.

Further study on the ensuing workload from the institution of SBOM as a required practice would not only provide these organizations with valuable information about the resources and time necessary for compliance, but it would also provide a realistic timetable to the NTIA for adopting and implementing regulations relating to SBOMs.

Automation Support

Regarding the automation support aspect of SBOM, as the NTIA notice points out, some of the difficulty with automating the generation, readability, and dissemination of SBOMs is the sheer scale of work that such an effort would take to standardize. As NTIA notes, there are already multiple questions and concerns with SBOMs that have not been addressed: multiple standards and practices across the industry regarding naming and categorizing software components[7]; automating the classification of older software (with fewer coding chains and embedded third-party software) will be hampered based on the outdated nature of this software, not to mention the possible inability to access relevant information about this software; and, as a last example, the nature of automating SBOM generation may itself be subject to vulnerabilities and tampering.

Automating the SBOM process, if done correctly, would provide an important and useful way to enhance the speed by which multiparty vulnerability coordination could occur. Even then, though, this automated process would still fail to offer the full information on exploitability in a

[7] https://www.nature.com/articles/s41746-021-00403-w

product that analysis by a skilled cybersecurity professional would provide. Through a study, the NTIA could better understand the likely synergy between an automated SBOM process and industry professionals who can analyze data from an SBOM, clarify whether vulnerabilities actually exist in a product, and create targeted next steps to publish and even rectify these vulnerabilities.

Limitations of Current SBOM Tools

In addition to pointing out opportunities for improvement in the NTIA's proposed guidelines, we also believe it is necessary to identify current shortcomings in current SBOM formats themselves. Two of the most widely used formats for developing SBOMs, Software Package Data eXchange (SPDX) and Software Identification (SWID), are currently unable to distinguish whether a software component has no further subcomponents or if it is unknown whether further subcomponents exist in said software. While it is difficult to comprehensively catalogue subcomponents on which there is little, if any, information, consumers should be able to know whether any "known unknowns" exist in a product to make an informed procurement decision.[8]

Further, CycloneDX, another popular SBOM format, does not natively address mapping vulnerabilities to supply chain components. A record of vulnerabilities is compiled separately into a "Vulnerability Exploitability" (VEX) report. This is both a positive and a negative: positive, in that such a report provides further details about a product's degree of vulnerability — instead of simply saying a product is vulnerable because it contains software X, VEX can clarify whether such software is exploitable based on its location/use in the product; negative, in that this may be an intensive and time-consuming resource for a downstream developer to produce (whether manually or through automation, both of which also present their own challenges).

We believe the NTIA should continue to collaborate closely with cyber professionals working on SBOM tools to identify opportunities for improvement, standardization, and streamlining. Such collaboration may shed light on new ways to improve existing SBOM formats and increase their usefulness to SBOM consumers. There are no automated tools that can perform a risk assessment based on any standardized version of SBOM. Without automated tools, the use of SBOMs in vulnerability coordination is of limited value at best, and it will prove to be a costly and time-consuming distraction at worst.

Conclusion

As such, we believe that further study is needed by the NTIA to elucidate multiple points prior to implementation of SBOMs: required data fields, the skill requirements and effort necessary to comply with the institution of SBOMs, and the likely breakdown of work between an automated process and human analysis.

With the already limited cybersecurity workforce, valuable time and resources may be spent complying with regulations that would currently do little to actually safeguard our supply chains. Data from such a study would provide a better understanding of what kind of information is (and is not) useful in an SBOM, how intensive it would be to comply with SBOMs for organizations, and whether more staff would be needed in these organizations for compliance.

[8] https://www.ntia.gov/files/ntia/publications/ntia_sbom_formats_and_standards_whitepaper_-_version_20191025.pdf

Introducing SBOMs as an industry standard is a worthy initiative for the cybersecurity world only after the necessary groundwork has been laid throughout both the public and private sectors to support multiparty vulnerability coordination. To make SBOM meet its potential, further study is needed to inform the true return on investment to ensure that its implementation actually solves software supply chain security problems, rather than simply creating another operational burden on an already overextended cyber workforce.

Sincerely,

Katie Moussouris

Katie Moussouris
Founder and CEO
Luta Security
www.LutaSecurity.com