DELL Technologies

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

Re: Software Bill of Materials Elements and Considerations (NTIA–2021–0001) – Comments of Dell Technologies, Inc.

Dear Acting Administrator Remaley:

Dell Technologies, Inc. ("Dell") respectfully submits the following comments in response to the National Telecommunications and Information Administration's ("NTIA") recent Request for Public Comment, 86 FR 29568 (Jun. 2, 2021) ("RFC"), concerning *Software Bill of Materials Elements and Considerations* (NTIA–2021–0001).

The use of Software Bill of Materials (SBOM) is an integral part of the Executive Order on Improving the Cybersecurity of the Federal Government, which will influence secure software development practices well beyond the Federal Government market. Securing the software supply chain is of critical interest to all purchasers and suppliers of software, including Dell. This comment responds specifically to the NTIA request for comments on SBOM elements, use cases, and related processes within the context of Dell's business objectives. It does not take into account the full state of all current research on SBOM and related concepts.

SBOM Costs and Benefits Must Be Carefully Weighed and Balanced

Dell understands the value of dependency management within the Secure Development frameworks that regulate and influence software development. It is important that software suppliers are fully knowledgeable of the components that comprise their offerings, proactively monitor those components for vulnerabilities, strive to address the vulnerabilities in a timely manner, and inform purchasers of those updates. These actions are the cornerstone of vulnerability management and are mandated in various standards and frameworks across the modern software ecosystem.

Dell believes a specific focus on SBOM as a quantum leap forward in maturity in third-party component management may, however, be misplaced. Recent high-profile supply chain attacks (e.g. Sunburst) would not have been detected or prevented with an SBOM. Rather, SBOMs constitute one technique in a mature organization's arsenal and are not a panacea for software vulnerabilities. Moreover, industry-wide deployment of SBOM will require significant investment beyond suppliers developing and issuing SBOMs. For example, widespread availability of SBOMs will likely require a government-led cross-industry educational initiative, as use of SBOMs without education on their use are highly likely to result in purchaser confusion.

Likewise, the SBOM contains version information relating to open-source components. This information, without additional context (e.g., back-ports of security fixes, compensating controls, or even component modification) can be misleading. Providing version information in some cases will add to purchaser confusion and supplier overhead. For example, a vendor may have customized a specific open-source component to fit its needs, as allowed by the license. Later, the vendor may backport a vulnerability fix to avoid having to customize a later version of the component. Describing these modifications in a manner which will educate purchasers, and not confuse them, may not be feasible.

Another implementation challenge is the role of contractual confidentiality restrictions imposed on commercially supplied components. SBOMs are often discussed in the context of open-source software components, but the NTIA proposal would extend to all software components. The inclusion of upstream commercial suppliers would raise several commercial challenges for suppliers. Of particular concern is that required elements of an SBOM may be subject to contractual confidentiality restrictions imposed by upstream suppliers. In the case of as-a-service offerings, commercial component information may even be considered trade secrets. Dell believes NTIA and the Department of Commerce must carefully consider the costs and realistic benefits of any detailed information requirements in SBOMs. Consideration of costs must also include opportunity costs. Any requirement that would require significant R&D and Customer Support investment could realistically come at the cost of other quality or security measures that may ultimately have a greater mitigating impact on the risks posed to purchasers.

The full costs of implementing detailed SBOM requirements should not be overlooked. Mature, enterprise-class tooling to enable complete SBOM identification (commercial and open-source) is still developing. Even when fully standardized, evaluation, procurement and incorporation of these tools across suppliers is a lengthy process requiring financial resources, dedicated staffing, and time. Until this happens, production of SBOMs by suppliers will likely involve significant manual effort by skilled experts whose time may be diverted from other quality and security initiatives, potentially resulting in a net negative in software quality and security.
We appreciate that the Federal Government has an opportunity here to influence the market and shift security maturity in the right direction for all purchasers. Using that ability responsibly in a way that allows suppliers the flexibility to adapt their processes and produce meaningful and accurate SBOMs without impacting other quality and security initiatives is in the best interest of both suppliers and purchasers.
.

Phased Approach to SBOM

Dell recommends limiting the information required to be disclosed in an initial implementation of SBOMs to a small amount of meaningful information, such as a list of all directly embedded open-source software component names. Over time, NTIA could add minimum or optional content requirements addressing more complex information. In this model, suppliers could still be required to collect additional information as they are able, but disclosure of that additional information it would be optional as an initial matter. To accomplish this, we recommend either a risk-based, tiered model, or a time-based phased model (or both).

In addition, for commercial suppliers not directly subject to the Executive Order, unless a contract is in place mandating the supply of an SBOM along with the component or requiring contract updates in the event of new regulatory requirements, there is no guarantee that suppliers to the government will be able to obtain an SBOM for some embedded components. Time is needed to allow companies to renegotiate contracts with such suppliers, and to allow those suppliers to renegotiate with their downstream suppliers, and so on. A tiered or phased approach would allow time for such contract renegotiations or renewals throughout the supply chain.

For example, a phased approach for SBOM implementation could follow these steps:

Phase 1: Listing the supplier and name of all direct (top-level) open-source dependencies **without** version, hash or other information
Phase 2: The above, adding commercially sourced components as permitted by contract
Phase 3: … adding version information when known
Phase 4: … adding whether and how the components were modified
Phase 5: … adding transitive dependencies for open-source components when known
Phase 6: … adding references to suppliers' SBOMs where the supplier has provided them
Phase 7: … adding transitive dependencies for commercial components where an SBOM has been provided by the supplier
(The trend here should be clear as maturity grows)

If these phases are viewed as tiers, it would also be possible to state that the SBOM for a specific version of a product achieves on-level/tier of SBOM maturity, whereas another product (or another version of the same product) does not.

Permitting a variety of tiers among SBOMs would give the purchaser more information about a supplier's offerings and allow purchasers to make risk-informed (and, if necessary, compliant)[1] procurement decisions. It also provides an approach that can be leveraged by suppliers to improve maturity of their SBOMs across their product lines over time. Lower-detail SBOMs can then be produced manually, and more detailed SBOMs developed over time as tooling and automation capabilities mature. It allows for suppliers to renegotiate contracts or find replacements for components that cannot be included in an SBOM. Finally, it gives room for the SBOM standard to grow over time by adding increasingly strict implementation phases, or more risk-averse tiers of compliance.

Responses to Specific Requests for Comment

1. SBOM Elements

While consensus has built among the NTIA working group for most SBOM elements, we recommend focusing on increasing supply chain transparency rather than adopting a

[1] For instance, a particular government agency may require that a supplier for a given use case be able to provide an SBOM of a specific level of detail depending on the risk associated with that use case.

compliance-based approach with respect to inclusion of these elements. Individual products and applications may be compliant with the SBOM standards to greater or lesser degrees and should not be subject to a strict "yes/no" certification of compliance. As a result, NTIA should clearly identify which elements are required and which are optional, ideally tied to the tiered/phased approach described above. This includes version, hash, and dependency information. Making certain elements optional will allow more suppliers to produce SBOMs and mature them over time.

It will be especially important that the purpose of the hash element be specified with precision. While we have no significant concerns with providing hashes of the components in software provided to a purchaser, we are concerned that a requirement to provide hashes of upstream components may cause confusion in instances where such components have been modified (as described further in the next section).

2. SBOM Use Cases

The following use cases reflect scenarios that may constitute gaps in the proposed definition.

Embedding a modified component
A component may be modified by rebuilding edited third-party source code, rebuilding the same third-party source code but with different tools, modifying compile-time or run-time configuration, removing unwanted subcomponents (or selecting only wanted subcomponents) and/or backporting security fixes from future versions. These actions are common in the industry and should be distinguishable by the purchaser from the creation of a forked version of the component. However, they do change how the SBOM element should be interpreted by the purchaser. While some of them may be able to be captured in the "dependency relationship" field, explicit standardization on capturing these modification types is needed and should take the input of both purchasers and suppliers into account.

Downstream restrictions and licenses
A supplier may wish to impose restrictions on who can receive a SBOM and who can share it further, which it may enforce with NDAs, contracts, copyrights or licenses. Metadata allowing documentation on SBOM sharing restrictions or IP protections are needed to reflect these restrictions.

Upstream legal obligations
A supplier may be subject to legal obligations on what it can disclose about an embedded component, including the manufacturer of the component (for example, an ODM "white label" arrangement where the contract prevents disclosure of the manufacturer). There may also be restrictions placed on a downstream purchaser by an upstream supplier on disclosing SBOM contents. It is unclear how to document components subject to these types of confidentiality restrictions.

* * *

These use cases highlight the need for requirements that support transparency but are not subject to a binary compliant/non-compliant assessment. Guidance on handling these scenarios is necessary, as they likely require flexibility in how SBOMs are constructed and

distributed. Suppliers may also need time to adjust how they bundle such offerings to minimize purchaser confusion.

3. SBOM-Related Processes

The following comments relate to certain SBOM-related processes referenced in the RFC.

b. Software-as-a-Service and Online Services
SaaS and online service offerings present different challenges than traditional on-premises product offerings. We believe that many SBOM use cases do not apply in the SaaS or online service offering context. Components in use for these offering types may change at any time with little or no visibility to end users, and responsibility for addressing vulnerabilities in such components is strictly held by the service provider. Unlike an on-premises product where the SBOM represents the known truth and will not change until explicit action is taken to update the product, a service offering's SBOM may change continuously, causing risk-based decision-making based on that SBOM difficult or even impossible. Finally, in a way which is fundamentally different from on-premises software, as-a-service offerings may incur additional security risks by disclosing implementation details or security controls through a SBOM.
We suggest that SBOM obligations for SaaS offerings be required only for the most critical software or at the highest tiers of maturity, if at all.

There are two additional complexities we associate with SaaS SBOMs:

- While it is challenging or impossible to keep a SBOM current in an environment where the offering is constantly changing, it is more complex when multiple versions of the offering are available simultaneously (such as in A/B testing or phased feature rollouts). In these situations, there may not be one "version" of the offering in use at any time, even perhaps in one user session.
- A service offering may rely on infrastructure components that might reasonably represent trade secrets which would not normally be disclosed in a SBOM.

c. Legacy and binary-only software
Suppliers may have no alternative but to embed components for which no verifiable information is available and for which the component supplier is no longer reachable. In these cases, suppliers should be able to note this without being "out of compliance" with the standards. A statement that the component cannot be analyzed further, or that some aspect of its provenance is unknown, must be allowed to enable to disclosure of "known unknowns."

f. High assurance use cases
While outside the scope of current approach, the SBOM documentation notes that "dependency relationship" may be used to capture dependencies beyond simple embedding of components. This may allow for capturing additional dependencies such as:

- Publicly (or privately-) available APIs the offering invokes;
- Components used to build or test the offering;
- Protocols and/or standards the offering leverages; or
- Runtime dependencies the offering requires.

This may allow for the use of an SBOM-derived document in handling the high-assurance use cases listed in the Executive Order. If this is the intent, further documentation of these use cases is required. If this is not the intent, new standards and specifications will be required. Tracking this type of dependency is not (yet) common practice, but we believe that suppliers who begin to adopt this practice will be better positioned to respond to reported vulnerabilities. This is another scenario where the tiered or phased approach to SBOM specification would be valuable in growing the maturity of the software development community.

g. Delivery
The SBOM delivery model should be flexible enough to allow for distribution only on-demand and only to specific purchasers, with restrictions on what a purchaser can do with the SBOM once acquired. Revision of SBOMs to correct errors or reflect new information is not covered in the RFC, but it is necessary that suppliers have the ability to publish new SBOMs in a way that make purchasers aware of incremental differences (for example, using a SBOM version identifier and/or publishing a summary of changes).

The metadata associated with assigning a delivery of a SBOM to a delivery of a software artifact is not fully defined. The association between the bits-on-hand for a given purchaser and the SBOM relevant to those bits must be unambiguous. Knowing (and proving) a SBOM and delivering a SBOM are two different tasks; some level of assurance should be recognized for suppliers whose SBOMs can be audited but who do not share them with all purchasers. It must be clear what the obligations or risks may be triggered by delivering a SBOM to a Federal Government purchaser who has obligations relating to public disclosure of records (e.g., FOIA).

h. Depth
The current model seems to require the SBOM author to fully expand all dependencies. An approach where a link or reference to another supplier's SBOM can be used instead would allow for a SBOM to improve over time as upstream suppliers mature their practices without putting a burden on downstream suppliers to constantly refresh their own SBOMs. A phased approach would allow some benefit from lower-detail SBOMs while the web of supplier SBOMs builds itself up over time.

At various depths of the dependency tree, it is also necessary to note that current dependency information is unreliable or that deeper dependency information is unavailable. In addition, we reiterate earlier statements about contractual obligations. Until SBOM clauses in procurement contracts become common, there will be SBOM elements which cannot be disclosed for legal reasons, or which are simply unknown.

i. Vulnerability and j. Risk Management
We believe vulnerability and risk information, including statements about false positives and non-exploitable vulnerabilities, belong in separate communication channels from the SBOM. The SBOM refers to a point in time, while vulnerability and risk information constantly changes. Additionally, successful use of vulnerability risk information requires a level of expertise. Suppliers already have means for sharing this information and handling customer support queries about it, which are mandated in standards like ISO/IEC 29147 and ISO/IEC 27001. A

shift in how this information is communicated would have a significant business impact on suppliers and could cause confusion among purchasers. It also introduces the potential for conflicting information between vendor-supplied security advisories, the National Vulnerability Database, and documentation like VEX.

4. Flexibility of Implementation

We are especially interested in how flexibility of implementation will be addressed in the implementation of the Executive Order as it relates to SBOM. Tiered or phased compliance with SBOM-related directives, as described above, will allow for much greater flexibility in how suppliers can approach SBOM requirements, maximizing benefits and compliance.
Of particular note is that it must be possible to leverage SBOM metadata to document the limits of a SBOM. This includes both limitations on the SBOM itself and limitations on specific elements within the SBOM. This gives the supplier more flexibility in how its offerings can be consumed, but also gives the purchaser the ability to make a more risk-informed decision on whether and how to use a supplied offering. We fundamentally believe it is more important to encourage and enable transparency in SBOMs than it is to enforce all-or-none compliance requirements.

We reiterate the comments made earlier in this document about the realities of contractual obligations within the software supply chain. Any proposal for compliance with SBOM directives must respect contractual obligations and the business reality of needing to cascade these obligations throughout the supply chain.

Conclusion

Dell embraces the importance of understanding and documenting a form of SBOM for its offerings to allow for more efficient vulnerability management and more informed risk-based procurement decisions by purchasers such as the Federal Government. However, the SBOM process must consider the realities of modern software production and distribution, including the prevalent modification of third-party components, the relative impact of SBOM on information security risk mitigation vis a vis alternative security investments, and the complexities of SBOM for software offered as a service.

Additionally, while we respect the importance of all suppliers being able to produce highly detailed SBOMs, the distribution of SBOMs to others must be handled carefully. Such requirements produce challenges for existing legal obligations around protecting trade secrets and other intellectual property.

We believe a tiered or phased approach to SBOM standards will best accommodate the implementation complexities discussed in these comments, as well as provide appropriate incentives for suppliers to mature their capabilities without losing access to the entire marketplace.