700 6th Street, N.W. Suite 400
Washington, DC 20001

bd.com

June 15, 2021

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave NW
Rm 4725
Washington, DC 20230
Attention: Evelyn L. Remaley

Via www.regulations.gov

RE: Docket No NTIA-2021-0001: Software Bill of Materials Elements and Considerations

Dear Sir/Madam,

We submit this letter on behalf of BD (Becton, Dickinson and Company). BD appreciates the opportunity to provide input related to the FR Notice, *Software Bill of Materials Elements and Considerations,* published by NTIA on June 2, 2021. We support NTIA's efforts for advancing transparency in the software supply chain by coordinating an open and transparent multistakeholder process that allows proposing solutions while unpacking challenges of software supply chain.

BD is one of the largest global medical technology companies in the world and is advancing the world of health by improving medical discovery, diagnostics and the delivery of care. BD helps customers enhance outcomes, lower costs, increase efficiencies, improve safety and expand access to health care.

BD would like to applaud the NTIA for proposing a set of minimum elements for a Software Bill of Materials (SBOM). BD very much appreciates the opportunity to share our views. Enclosed are our comments for consideration.

Should you have any questions or comments, please contact Jeff Ballyns at 202-777-1587 or Jeffrey.Ballyns@bd.com.

Best regards,

/s/

Jeff Ballyns, Ph.D.
Associate Director, Regulatory Policy
Public Affairs

CC: Fatemeh Razjouyan, Director, Regulatory Policy; Dana-Megan Rossi, Director, Information Security; Mike Pieper, Cybersecurity Officer EMEA

#	Question/Location	Comment/Proposed Change	Rationale
1	Are the elements described above, including data fields, operational considerations, and support for automation, sufficient? What other elements should be considered and why? *Page 29570 - Docket No. 210527-0117*	The data fields "baseline component information" are sufficient. Considering the current lack of maturity within the industry (SBOM author & recipient) and SBOM automation vendors, it is not opportune to go beyond these baseline attributes.	It should be taken into account that even baseline attributes can be difficult to obtain, as the SBOM author depends on the quality of information upstream. Examples include: the lack of a central repository for software component identification; no uniform international identification standards software developers adhere to; lacking visibility of third-party component relationships and depth.
2	Are there additional use cases that can further inform the elements of SBOM? *Page 29570 Docket No. 210527-0117*	If risk and vulnerability management is the main purpose of the SBOM, the baseline component attributes will suffice for proper identification of the component.	
3a	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. *Page 29570 Docket No. 210527-0117*	SBOM authors are dependent on the identifier attribute provided by the developer/publisher of the third-party software component. Without an international accepted (regulated) standard, this will not change on short term. "Best effort" should be the short-term goal.	
3b	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	Identifying cloud services for SBOM is challenging. Cloud services in use by a product can go beyond SAAS and could include (shared) PAAS, IAAS and hybrid solutions. This includes API's and any other software in use on those	Without (enforceable) requirements to the SBOM for cloud service providers, incorporating comprehensive cloud service identification in the downstream SBOMs is

	that is not running on customer premises or maintained by the customer. *Page 29570 Docket No. 210527-0117*	platforms. These services are usually prone to continuous change and the user of these services is not always informed appropriately on these changes.	limited to what is currently provided by such vendors.
3c	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. *Page 29570 Docket No. 210527-0117*	Legacy software can be noted as such in the SBOM together with the limited attributes that are available for the specific binary.	
3d	Integrity and authenticity: An SBOM consumer may be concerned about verifying the source of the SBOM data and confirming that it was not tampered with. Some existing measures for integrity and authenticity of both software and metadata can be leveraged. *Page 29570 Docket No. 210527-0117*	Digital signing can be leveraged to ensure integrity and authenticity, if supported on the document exchange format and the author of the SBOM has the means and capabilities.	
3e	Threat model: While many anticipated use cases may rely on the SBOM as an authoritative reference when evaluating external information (such as vulnerability reports), other use cases may rely on the SBOM as a foundation in detecting more sophisticated supply chain attacks. These attacks could include compromising the integrity of not only the systems used to build the software component, but	No additional comments.	

	also the systems used to create the SBOM or even the SBOM itself. How can SBOM position itself to support the detection of internal compromise? How can these more advanced data collection and management efforts best be integrated into the basic SBOM structure? What further costs and complexities would this impose? *Page 29570 Docket No. 210527-0117*		
3f	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? *Page 29570 Docket No. 210527-0117*	For high assurance cases, additional attributes can be added to the software component including supplier name, environment name and version number of the development, and build environment.	
3g	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. *Page 29570 Docket No. 210527-0117*	Automated SBOM exchange between author and recipient in a machine-readable format is highly unfeasible in the short to mid-term due to the lack of maturity in the industry, lack of maturity in SBOM automation vendors, lack of internationally recognized standards in terms of component identification, and SBOM format. Both author and recipient of SBOMs will need to invest in setting up internal processes, resources, IT infrastructure, and software tools.	

3h	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. *Page 29570 Docket No. 210527-0117*	As this is an issue indeed, we recommend limiting the minimum depth of one layer, or the deepest layer capable of being produced until the industry matures.	
3i	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. *Page 29570 Docket No. 210527-0117*	We agree that including vulnerability information in the SBOM is not ideal as vulnerability information changes over time and could result in recipients referring to out-of-date SBOM versions. Instead, it is recommended to not include vulnerability information in the SBOM document but leave vulnerability and risk management up to the author and recipient of the SBOM. New vulnerabilities should be communicated to recipients via coordinated vulnerability disclosures.	
3j	Risk Management. Not all vulnerabilities in software code put operators or users at real risk from software built using those vulnerable components, as the risk could be mitigated elsewhere or deemed to be negligible. One approach to managing this might be to communicate that software is "not affected" by a specific vulnerability through a Vulnerability Exploitability exchange (or "VEX"),14 but other solutions may exist. *Page 29570 - Docket No. 210527-0117*	Coordinated Vulnerability Disclosure on product level might be a more suitable direction to disclose any vulnerabilities in the product, the eventual risk for the user of the product and what mitigations can / are being taken to reduce risk. The SBOM is not the most appropriate "vehicle" for this.	

4	Flexibility of implementation and potential requirements. If there are legitimate reasons why the above elements might be difficult to adopt or use for certain technologies, industries, or communities, how might the goals and use cases described above be fulfilled through alternate means? What accommodations and alternate approaches can deliver benefits while allowing for flexibility? *Page 29570 - Docket No. 210527-0117*	Implementation should remain flexible considering the challenges SBOM authors and recipients are still facing. An acknowledged international (IEC/ISO) SBOM standard will likely aid in overcoming the issues currently at hand.	