Before the Department of Commerce
National Telecommunications and Information Administration
Washington, D.C.

In The Matter of

Software Bill of Materials Elements and Considerations	)	NTIA-2021-0001
	)	Docket No. 210527-0117
	)	

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Assistant Vice President, Cybersecurity & Privacy

Avonne Bell
Director, Connected Life

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

June 17, 2021

Table of Contents

I. INTRODUCTION

CTIA[1] welcomes the opportunity to comment on the National Telecommunications and Information Administration's ("NTIA") request for comment, *Software Bill of Materials Elements and Considerations* ("RFC").[2] President Biden's Executive Order on Improving the Nation's Cybersecurity ("Cyber EO")[3] defines a Software Bill of Materials ("SBOM") as a "formal record containing the details and supply chain relationships of various components used in building software."[4] NTIA's RFC proposes a set of minimum elements for a model SBOM[5] and seeks comment on additional questions.[6]

CTIA supports the broad goals of the Cyber EO and believes that SBOMs can help the Federal Government to enhance its cybersecurity posture. The wireless sector uses SBOMs and associated tools to onboard, evaluate, test, and deploy software in networks and in solutions for customers. NTIA and other agencies, like the National Institute of Standards and Technology ("NIST"), have an opportunity with this proceeding and related work to help federal agencies develop workable SBOM expectations for government contractors selling software to the government. The evolution of SBOM will be ongoing—the government and private sector must work together and refine approaches. The present proceeding should reflect that need.

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, and suppliers, as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Software Bill of Materials Elements and Considerations, 86 Fed. Reg. 29,568 (May 27, 2021) ("RFC").

[3] Exec. Order No. 14,028, 86 Fed. Reg. 26,633, at Section 4(f) (May 17, 2021) ("Cyber EO").

[4] *Id.* at Section 10(j).

[5] *See* RFC at 29,569.

[6] *See id.* at 29,570.

II. NTIA'S WORK UNDER THE CYBER EO WILL HAVE IMPORTANT CONSEQUENCES

The Cyber EO directs the Secretary of Commerce, with the Assistant Secretary for Communications and Information and the Administrator of NTIA, to publish minimum elements for an SBOM.[7] This directive is part of Section 4 of the Cyber EO, which aims to enhance the security of the software supply chain.[8]

Section 4 of the Cyber EO provides that "[t]he security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions."[9] The Cyber EO identifies "a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended."[10] Specifically, the integrity of "critical software"—which the Cyber EO describes as "software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access)"—"is a particular concern."[11]

In light of this, the Cyber EO mandates three key government actions with respect to critical software. First, it directs the Secretary of Commerce, through the Director of NIST, to define "critical software"[12] for inclusion in guidance "identifying practices that enhance the security of the software supply chain."[13] Second, the Cyber EO directs the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security

[7] Cyber EO at Section 4(f).
[8] *See id.* at Section 4.
[9] *Id.* at Section 4(a).
[10] *Id.*
[11] *Id.*
[12] *Id.* at Section 4(g) (citing to Section 4(e)). This definition "shall reflect the level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised." *Id.*
[13] *Id.* at Section 4(e). Among other things, this guidance shall include standards, procedures, or criteria regarding "providing a purchaser [an SBOM] for each product directly or by publishing it on a public website." *Id.* at Section 4(e)(vii).

Agency ("CISA") and in consultation with the Secretary of Commerce acting through the Director of NIST, to "identify and make available to agencies a list of categories of software and software products in use or in the acquisition process" that meet NIST's definition of "critical software."[14] Third, the Cyber EO requires the Secretary of Commerce, through NIST and others, to "publish guidance outlining security measures for critical software[,] . . . including applying practices of least privilege, network segmentation, and proper configuration."[15]

NTIA's work on SBOM will play an important role under the Cyber EO in helping to secure the supply chain for software used by the Federal Government, especially when it comes to critical software. To fulfil its obligation under the Cyber EO, NTIA appears to be accelerating its prior work on SBOM into a baseline that may become a set of mandatory requirements. NTIA's prior work consists of voluntary tools that are the product of multistakeholder input.

NTIA's acceleration of that work can expedite the evolution of SBOMs. However, this expansion of SBOMs must be an evolving process as organizations consider how to build, communicate, and use them. As such, NTIA should make sure that agencies do not think of this SBOM initiative as a static or one-time effort. NTIA should take a targeted approach and heed all feedback, because stakeholders that were previously uninvolved in NTIA's SBOM work are now evaluating NTIA's proposals.

III. NTIA HAS IDENTIFIED THE RIGHT BUILDING BLOCKS THAT CAN HELP FEDERAL AGENCIES MANAGE SBOMS

In the RFC, NTIA proposes a definition of the "minimum elements" of an SBOM that "builds on three broad, inter-related areas: Data fields, operational considerations, and support

[14] *Id.* at Section 4(h).
[15] *Id.* at Section 4(i).

for automation."[16] The RFC seeks comment on whether these elements are sufficient and whether other elements should be considered.[17] As noted, SBOM has been a work in progress at NTIA and existing SBOM elements have resulted from NTIA's multistakeholder process. While the definition of minimum proposed SBOM elements identifies the building blocks that may help agencies manage SBOMs, the development of SBOMs will be a journey for industry stakeholders. And although government contractors will feel the impact of NTIA's decisions acutely, the software ecosystem as a whole will be affected as well.

A. NTIA can champion flexible operational considerations for a model SBOM

The RFC explains that "[e]lements of SBOM include a set of operational and business decisions and actions that establish the practice of requesting, generating, sharing, and consuming SBOMs."[18] According to NTIA, this includes: (1) frequency; (2) depth; and (3) delivery.[19] CTIA urges NTIA to embrace flexibility in determining these operational considerations in particular, and also as a fundamental aspect of a model SBOM overall.

The RFC notes that "[s]oftware is made and used by a wide range of organizations, but this diversity makes a single model for SBOM difficult."[20] The RFC also points out that "SBOM practices are still novel in some communities."[21] CTIA urges NTIA to expand upon the diversity of software in today's landscape and the challenges it poses for the development of a single SBOM model. NIST and NTIA should emphasize this point if they advise the Federal Acquisition Regulatory ("FAR") Council on SBOM requirements for government contractors. Ultimately, NTIA and the federal procurement system should approach SBOM minimum

[16] RFC at 29,569.
[17] *Id.* at 29,570.
[18] *Id.* at 29,569.
[19] *See id.*
[20] *Id*.
[21] *Id.*

elements in a tailored way, so that the complexities that inevitably arise in developing minimum elements can be addressed and resolved, and unnecessarily burdensome obligations for government contractors or other members of the private sector can be avoided.

CTIA addresses each of the specific operational considerations in the RFC as follows:

1. Frequency

Through its multistakeholder process, NTIA has specified that the generation frequency for an SBOM should be "[w]ith every update or change to code[,]" be it a major or a minor release or patch.[22] The RFC echoes this point.[23] Although, as noted above, CTIA believes that flexibility on NTIA's part will be a key component of the successful development of the operational considerations element of a model SBOM, CTIA agrees with NTIA that to be effective an SBOM will likely need to be generated for each patch or update to software. This may create operational challenges for companies and may support deploying SBOMs in a way tailored to software procurements so that complexities can be evaluated and adjusted for.

2. Depth

The RFC asserts that "[t]he ideal SBOM should track dependencies, dependencies of those dependencies, and so on down to the complete graph of the assembled software[,]" and should acknowledge any "known unknowns."[24] The appropriate level of depth for an SBOM may vary depending on the software or setting in question. As such, CTIA urges NTIA to encourage flexibility by agencies in determining how deep a model SBOM will go.

[22] NTIA, SBOM Options and Decision Points, at 2 (last revised Apr. 27, 2021), https://www.ntia.gov/files/ntia/publications/sbom_options_and_decision_points_20210427-1.pdf ("SBOM Options and Decision Points").

[23] *See* RFC at 29,569 ("A new build or an update to the [software's] underlying source should, in turn, create a new SBOM.").

[24] *Id*.

3. Delivery

NTIA's RFC acknowledges that "there will not be a one-size-fits-all approach" to the delivery of SBOMs.[25] As NTIA explains, "SBOMs should be available in a timely fashion to those who need them and have proper access permissions and roles in place."[26] The RFC also seeks comment on other mechanisms that could be used to deliver SBOM data.[27]

NTIA has previously observed that SBOMs should be "[b]undled with every product version and archived by the supplier."[28] Efforts are underway at the Internet Engineering Task Force (IETF) to specify "different means for SBOMs to be retrieved[,]" including on devices themselves, via website URL, and through some form of out-of-brand contact with the supplier.[29] In line with the flexibility that CTIA urges NTIA to embrace, CTIA supports varied methods for delivering SBOM information—like the means put forth by the IETF—and recommends that NTIA consider these means of delivery as well in determining the minimum SBOM elements.

Further, NTIA, NIST, or other managers of SBOM communication must ensure that the manner of delivery it ultimately chooses to embrace enables the secure transfer, receipt, and storage of, and access to, an SBOM while it is in transit, at rest, and in use. The SBOM delivery process must be built upon a foundation of confidentiality, authentication, integrity, and non-repudiation. CTIA recommends that this foundation be embodied in contractual terms governing the SBOM delivery process, although the development of standards that could be referenced in the contract would enhance the delivery process as well. Additionally, NTIA should consider

[25] *Id.* The RFC specifies that "[e]xecutables that live on endpoints can store the SBOM data on disk with the compiled code, whereas embedded systems or online services can have pointers to SBOM data stored online." *Id.* at 29,569-70.

[26] RFC at 29,569.

[27] *Id.* at 29,570.

[28] SBOM Options and Decision Points at 2.

[29] IETF, Discovering and Accessing Software Bills of Materials, at 1 (May 18, 2021), https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-sbom-access.

using digital signing authorities with public X.509 certificates to authenticate the source of an SBOM. The Linux Foundation, for example, supports trusted signing for all projects under their umbrella.[30]

B. NIST can help NTIA develop data fields identified in the RFC

CTIA generally agrees with the "baseline component information" that the RFC lays out to comprise the data fields element of the proposed minimum SBOM. However, CTIA recommends that, as its work on SBOMs evolves, NTIA coordinate with and rely on NIST to consider requirements associated with baseline components as they apply to federal agency procurement. Given its statutory directives to develop federal IT standards—under the Federal Information Security Modernization Act ("FISMA"), for instance—NIST will be well positioned to help agencies consider contract requirements or other technical specifications when it comes to SBOMs.[31]

The RFC establishes the following categories of baseline component information: (1) supplier name; (2) component name; (3) version of the component; (4) cryptograph hash of the component; (5) any other unique identifier; (6) dependency relationship; and (7) author of the SBOM data.[32] The RFC adds that "[s]ome of these data fields"—like the dependency relationship field—"could be expanded[,]" and that "[o]ther data fields may need more clarity, including data fields for component and supplier name."[33]

[30] *See* Press Release, The Linux Foundation, Linux Foundation Announces Free sigstore Signing Service to Confirm Origin and Authenticity of Software (Mar. 9, 2021), https://www.linuxfoundation.org/en/press-release/linux-foundation-announces-free-sigstore-signing-service-to-confirm-origin-and-authenticity-of-software/.
[31] *See* Federal Information Security Modernization Act, 44 U.S.C. § 3551 *et seq.*
[32] RFC at 29,569.
[33] *Id.*

Based on members' experience using SBOMs, CTIA offers observations for NTIA to consider as it develops guidance for government software acquisitions. As an initial matter, CTIA believes that the minimum data fields for a model SBOM should ultimately include, at the very least, supplier name, component name, and version of the component. Additionally, if an SBOM includes vulnerability data, it must also include a data field containing the source of the vulnerability data and the date on which the SBOM was created. In the case of known vulnerabilities, an indicator should be included in the SBOM data model, along with directions to the test or analysis that proves that the vulnerability is ineffective, or to mitigating controls. Beyond these considerations, however, there are five additional data fields that CTIA believes may make a model SBOM more useful.

First, a data field could be established for the origin of the software component, which would differ from and expand upon the mere name of the software's supplier. Second, NTIA could include component license information and a time stamp for that information—such a time stamp could be an asset given that an SBOM is really a snapshot of the software in question at a given time. Third, it may be useful to include a runtime comparison of the SBOM to the software that is ultimately delivered or a framework that can be used to do so. Fourth, with regard to open-source software packages, it could be helpful to include a list of contributors and their countries of origin.[34] Fifth, and finally, because the names of the software component packages that are bundled in object code are usually different than the actual names collected from the package managers in the source code, it may be beneficial to have an optional field for a component's alias.

[34] However, country of origin information may only be obtainable for code produced by open-source communities where contributors are registered, such as those managed by the Linux Foundation.

With regard to the proposed sixth category of baseline component information above, focusing on the *position* of various components rather than their *relationships* may yield better results given the inherent difficulties in identifying software relationships. Perhaps more importantly, CTIA notes some of the data fields that the RFC proposes have not been fully developed in NTIA's multistakeholder process, and these data fields may benefit from NIST's input. The data fields in the RFC appear to build on data fields that were addressed in NTIA's multistakeholder process,[35] but for which there are not specified requirements. In particular, NTIA has acknowledged difficulties in developing a software identification solution.[36] As a result, NTIA is yet to provide additional specifications for what will be required of the "cryptograph hash of the component" data field. Meanwhile, NIST has signaled approval for certain hash algorithms[37] and may be a helpful resource in this context, particularly as quantum computing-enabled threats emerge. As such, CTIA recommends that NTIA work with NIST to specify associated requirements for the RFC's baseline component information—like the requirements for a component hash—in a draft special publication to be distributed for public comment.

C. Automation of SBOMs requires further collaboration

The RFC explains that "[a] key element for SBOM to scale across the software ecosystem, particularly across organizational boundaries, is support for automation, including

[35] *See* SBOM Options and Decision Points; NTIA, Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM) (Nov. 12, 2019), https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf (establishing largely the same data fields as the RFC).

[36] *See* NTIA, Software Identification Challenges and Guidance, at 10 (Mar. 30, 2021), https://www.ntia.gov/files/ntia/publications/ntia_sbom_software_identity-2021mar30.pdf ("Further work is needed to design, test, and implement global software component and supplier identification.").

[37] *See* NIST, FIPS 180-4, *Secure Hash Standard* (Aug. 2015), https://csrc.nist.gov/publications/detail/fips/180/4/final; NIST FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions* (Aug. 2015), https://csrc.nist.gov/publications/detail/fips/202/final.

automatic generation and machine readability."[38] This echoes the Cyber EO's definition of an SBOM, which provides, in part, that "[a] widely used, machine-readable SBOM format allows for greater benefits through automation and tool integration."[39]

CTIA agrees with the RFC and the Cyber EO on this goal, but it is important to note that automation for SBOMs is a work in progress. As the RFC explains, "[t]he SBOM community has identified three existing data standards" or formats "that can convey the data fields and be used to support the operations" the RFC describes.[40] These formats are (1) SPDX; (2) CycloneDX; and (3) SWID tags. The RFC asserts that "[b]ecause these formats already are subject to public input and translation tools exist, they serve as logical starting points for sharing basic data."[41] Each of these formats have advantages and disadvantages. However, from an automation standpoint, what will be most important going forward is ensuring that software composition analysis software is able to consume an SBOM and compare it to a vulnerability database, while providing a date of the most recent update to the vulnerability database.

IV. NTIA CAN HELP AGENCIES CONSIDER HOW THEY WILL USE SBOM INFORMATION

This proceeding is one step in an ongoing evolution in the SBOM area. As SBOM use becomes more widespread, government agencies will confront practical questions as they take in more SBOM information. NTIA, or perhaps more appropriately, NIST, can help agencies address the operational considerations that may arise, and the sooner they do so the better. Looking ahead, it would be a significant help to agencies if NTIA and NIST promote a tailored approach that enables agencies to ease into SBOM management and use. In particular, CTIA

[38] RFC at 29,570.
[39] Cyber EO at Section 10(j).
[40] RFC at 29,570.
[41] *Id.*

believes that there are three issues that could challenge agencies as they begin to work with SBOM information.

A. The use and ingestion of SBOM information will require care

Agencies will need to consider how they will ingest and use SBOM information. In particular, if the government mandates the use of SBOMs for contractors, it will have to clarify how the government will process the SBOM information it receives from its contractors, and how it will put that SBOM information to use. This will include determining whether the government intends to centralize the SBOM information it receives from its contractors and share it with other agencies. NIST may need to assist agencies in making these determinations, so NTIA should identify this as a consideration going forward.

Further, while CTIA supports various methods of SBOM delivery, the manner of delivery for mandated SBOMs must be made clear for the sake of efficiency and transparency. In other information sharing scenarios—including the sharing of threat indicators[42] and proprietary information of critical infrastructure operators[43]—the government has taken care to ensure that information is not used for purposes unrelated to its collection, regulatory or otherwise. Thus, NTIA should urge agency users of SBOMs to specify how government expects to use the SBOM information it receives from its contractors.

B. Agencies must consider how to secure and protect SBOM information

Agencies should consider how SBOM information will be secured and protected from broad dissemination and acquisition by bad actors, and NTIA should assist agencies in this. As CTIA noted, the wireless industry uses SBOMs and associated tools, but the information that

[42] *See* The Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501-1510.

[43] *See* 6 C.F.R. pt. 29.

comprises these SBOMs is protected by manufacturers and is generally unavailable to the public. Depending upon the contractor, the SBOM that may be provided to the government could consist of sensitive, proprietary information. As such, agencies must assess how they will authorize privileged access to this information. Contractors need to know who, if anyone, beyond the government personnel responsible for the contract will have access to the contractor's SBOM information. Ensuring the secure, controlled distribution of this information will avoid potential issues for contractors that could arise as a result of the widespread disclosure of the contractor's SBOM information.

If the evolution of SBOMs is to continue smoothly, the private-public partnership that the Cyber EO calls for must be paramount.[44] Looking ahead, NTIA and NIST can foster this partnership by helping agencies to determine how they will secure and protect the SBOM information they receive.

C. Agencies' work with SBOMs should reflect risk-based prioritization

Agencies will need to base their collection, ingestion, and use of SBOM information on the risk for which the SBOM information is sought. Otherwise, agencies may be overwhelmed by the volume of SBOM information they receive, much of which may ultimately be unhelpful.

As the RFC notes, "[n]ot all vulnerabilities in software code put operators or users at real risk from software built using those vulnerable components . . . ."[45] CTIA agrees with the RFC that not all vulnerabilities are the same—the information necessary to resolve one vulnerability may be far more than is necessary to resolve another. Ultimately, the most significant benefit of

[44] *See* Cyber EO at Section 1 ("Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector.").

[45] RFC at 29,570. The RFC notes that "[o]ne approach to managing this[,]" among others, "might be to communicate that software is 'not affected' by a specific vulnerability through a Vulnerability Exploitability eXchange . . . ." *Id.*

an SBOM is its ability to provide software owners and operators with information about a vulnerability that may exist in their software once that vulnerability is discovered. However, the provision of information beyond that which pertains to the relevant vulnerability should neither increase nor decrease the efficacy of an SBOM as a means to address a newly discovered risk. NTIA may want to emphasize this to agencies and ensure that SBOMs only need to provide the information necessary to combat the risk at hand.

V. NTIA SHOULD HELP THE FAR COUNCIL AND OTHER AGENCIES TAILOR SBOMS FOR CONTRACTORS SELLING SOFTWARE PRODUCTS TO THE FEDERAL GOVERNMENT

It is important that any SBOM requirements that result from NTIA's work under the Cyber EO focus on software products that the government acquires for its own use. SBOM procurement obligations of the sort envisioned by the Cyber EO do not extend, for example, to software that contractors may use within their own information systems. The RFC provides that "SBOM creation and use touches on a number of related areas in IT management, cybersecurity, and public policy[,]" and seeks comment on "how these issues . . . should be considered in defining SBOM elements today and in the future."[46] However, a contractor's own networking functions and services—such as network, cloud, and hosting services—are clearly outside the scope of any SBOM requirements for contractors, as contemplated by the Cyber EO. Similarly, customer premises equipment and end user equipment like smartphones, tablets, and connectivity products that the government purchases from commercial entities are not the sort of procurements subject to SBOM obligations under the Cyber EO. Such products are maintained and managed by manufacturers, application developers, and carriers to varying degrees and are not suitable candidates for SBOM obligations.

[46] *Id.*

The Cyber EO contemplates a narrow approach in which SBOM obligations flow to entities that sell software directly to the government. NTIA should explicitly recognize this now, in order to prevent its SBOM work from being prematurely extrapolated to broader settings.

Section 4 of the Cyber EO focuses on "software *used* by the Federal Government[,]" and this focus manifests itself in five paragraphs in Section 4.[47] First, Paragraph (h) directs the Secretary of Homeland Security, acting through the Director of CISA, to "identify and make available to agencies a list of categories of software and software products *in use or in the acquisition process*" that meet NIST's forthcoming definition of "critical software."[48] Second, Paragraph (k) instructs the Office of Management and Budget's ("OMB") Administrator of the Office of Electronic Government ("OEG") to ensure "that agencies comply with [the NIST guidance required by Section 4(e)] with respect to software *procured* after the date of this order."[49] Third, Paragraph (n) requires the Secretary of Homeland Security to "recommend to the FAR Council contract language requiring suppliers of software *available for purchase by agencies*" to comply with the requirements in Section 4(g)-(k) of the Cyber EO.[50] Fourth, Paragraph (p) requires agencies to "remove *software products*" that do not meet the new requirements adopted pursuant to Section 4(n) from all government-wide and multiple-agency contracts from which the government may purchase software products (such as General Services Administration schedule contracts).[51] Fifth, and finally, Paragraph (q) directs the OMB's OEG to "require agencies *employing software* developed and *procured* prior to the date of this order,"

[47] Cyber EO at Section 4(a) (emphasis added).
[48] *Id.* at Section 4(h) (emphasis added).
[49] *Id.* at Section 4(k) (emphasis added).
[50] *Id.* at Section 4(n) (emphasis added).
[51] *Id.* at Section 4(p) (emphasis added).

including agencies seeking to renew "software contracts," to either "comply with any requirements issued pursuant to [Paragraph] (k) of [Section 4]" or provide a plan for doing so.[52]

Each of these provisions relates to the government's acquisition and subsequent *use* of software products. This is underscored by the fact that FAR 2.101 defines "acquisition" to mean "the acquiring by contract with appropriated funds of supplies or services . . . *by and for the use of the Federal Government* through purchase or lease . . . ."[53] While the scope of this definition could include software products supplied to the government indirectly—such as software acquired from a subcontractor and delivered to the government, either as a stand-alone product or as part of an integrated software system, as well as software sold to the government through a reseller—it would not include software products used by contractors to perform government work. The same should be true for any SBOM requirements that ultimately flow from NTIA's work under the Cyber EO.

In the coming years, parts of the government may consider expanding SBOM obligations to regulated entities or applying it to contracts beyond software purchases. NTIA should recognize this and be explicit that the minimum SBOM elements it is developing are focused on federal agency procurement of software products. After all, contractors who perform services for the government, or deliver non-software products to the government, will have other cybersecurity obligations to meet, apart from those in Section 4 of the Cyber EO.[54] Indeed, other parts of the Cyber EO contemplate additional cyber standards for government contractors.[55]

[52] *Id.* at Section 4(q) (emphasis added).

[53] 48 C.F.R. § 2.101.

[54] For example, Department of Defense contractors are already subject to the obligations in DFARS Clause 252.204-7012, and the Cybersecurity Maturity Model Certification ("CMMC") program's requirements continue to evolve. *See* DFARS Case 2019-D041, 85 Fed. Reg. 61,505 (Sept. 29, 2020) (issuing interim rule to implement CMMC framework and inviting public comment on formation of the final rule).

[55] *See, e.g.,* Cyber EO Section 2(b), (g)(i)(D), (F), and (h)(i).

Ultimately, agency standards-setting and recommendation processes, especially the FAR Council process, must have substantial opportunity for input from the private sector and contractors. In adopting minimum SBOM elements, NTIA should clarify that any application of these minimum elements should be reserved for situations in which contractors are selling software directly to the government, and that any applications outside of this context will be determined through independent proceedings, subject to participation from industry stakeholders.

VI. CONCLUSION

CTIA supports SBOMs and their continued development, because they can play an important role in federal agencies' cybersecurity. This proceeding is an early step in what will be a gradual evolution—an evolution in which NTIA and NIST can help agencies manage risk by promoting SBOM practices that are risk-based, manageable, and secure. In doing so, NTIA can help the government provide predictability to entities selling software products to the government by clarifying the scope of their obligations.

Respectfully submitted,

/s/ *Melanie K. Tiano*_
Melanie K. Tiano
Assistant Vice President, Cybersecurity & Privacy

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Avonne Bell
Director, Connected Life

June 17, 2021