Scientific and Statistical Committee—8 a.m.

Day 4—Thursday, June 24, 2021

California State Delegation—7 a.m.
Oregon State Delegation—7 a.m.
Washington State Delegation—7 a.m.
Coastal Pelagic Species Advisory Subpanel—8 a.m.
Coastal Pelagic Species Management Team—8 a.m.
Groundfish Advisory Subpanel—8 a.m.
Groundfish Management Team—8 a.m.
Highly Migratory Species Advisory Subpanel—8 a.m.
Highly Migratory Species Management Team—8 a.m.
Scientific and Statistical Committee—8 a.m.
Enforcement Consultants—As Necessary

Day 5—Friday, June 25, 2021

California State Delegation—7 a.m.
Oregon State Delegation—7 a.m.
Washington State Delegation—7 a.m.
Coastal Pelagic Species Advisory Subpanel—8 a.m.
Coastal Pelagic Species Management Team—8 a.m.
Groundfish Advisory Subpanel—8 a.m.
Groundfish Management Team—8 a.m.
Highly Migratory Species Advisory Subpanel—8 a.m.
Highly Migratory Species Management Team—8 a.m.
Enforcement Consultants—As Necessary

Day 6—Saturday, June 26, 2021

California State Delegation—7 a.m.
Oregon State Delegation—7 a.m.
Washington State Delegation—7 a.m.
Groundfish Advisory Subpanel—8 a.m.
Groundfish Management Team—8 a.m.
Enforcement Consultants—As Necessary

** No Meetings Scheduled for Sunday, June 27, 2021*

Day 7—Monday, June 28, 2021

California State Delegation—7 a.m.
Oregon State Delegation—7 a.m.
Washington State Delegation—7 a.m.
Groundfish Advisory Subpanel—8 a.m.
Groundfish Management Team—8 a.m.
Enforcement Consultants—As Necessary

Day 8—Tuesday, June 29, 2021

California State Delegation—7 a.m.
Oregon State Delegation—7 a.m.
Washington State Delegation—7 a.m.
Groundfish Advisory Subpanel—8 a.m.
Groundfish Management Team—8 a.m.
Enforcement Consultants—As Necessary

Day 9—Wednesday, June 30, 2021

California State Delegation—7 a.m.
Oregon State Delegation—7 a.m.
Washington State Delegation—7 a.m.

Although non-emergency issues not contained in this agenda may come before the Pacific Council for discussion, those issues may not be the subject of formal Council action during this meeting. Council action will be restricted to those issues specifically listed in this notice and any issues arising after publication of this notice that require emergency action under section 305(c) of the Magnuson-Stevens Fishery Conservation and Management Act, provided the public has been notified of the Pacific Council's intent to take final action to address the emergency.

Special Accommodations

Requests for sign language interpretation or other auxiliary aids should be directed to Mr. Kris Kleinschmidt at (503) 820–2412 at least 10 business days prior to the meeting date.

Authority: 16 U.S.C. 1801 *et seq.*

Dated: May 27, 2021.

Tracey L. Thompson,

Acting Deputy Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2021–11547 Filed 6–1–21; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 210527–0117]

RIN 0660–XC051

Software Bill of Materials Elements and Considerations

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice, request for public comment.

SUMMARY: The Executive Order on Improving the Nation's Cybersecurity directs the Department of Commerce, in coordination with the National Telecommunications and Information Administration (NTIA), to publish the minimum elements for a Software Bill of Materials (SBOM). Through this Notice, following from the Executive Order, NTIA is requesting comments on the minimum elements for an SBOM, and what other factors should be considered in the request, production, distribution, and consumption of SBOMs.

DATES: Comments are due on or before June 17, 2021.

ADDRESSES: Written comments may be submitted on this document identified by NTIA–2021–0001 through *www.regulations.gov* or by email to *SBOM_RFC@ntia.gov*. Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Room 4725, Attn: Evelyn L. Remaley, Acting NTIA Administrator, Washington, DC 20230. For more detailed instructions about submitting comments, see the ''Instructions for Commenters'' section at the end of this Notice.

FOR FURTHER INFORMATION CONTACT: Allan Friedman, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Room 4725, Washington, DC 20230; telephone: (202) 482–4281; email: *afriedman@ntia.gov.* Please direct media inquiries to NTIA's Office of Public Affairs: (202) 482–7002; email: *press@ntia.gov.*

SUPPLEMENTARY INFORMATION:

Background

On May 12, 2021, the President issued Executive Order 14028, ''Improving the Nation's Cybersecurity.'' [1] An initial step towards the Executive Order's goal of ''enhancing software supply chain security'' is transparency. As the Order itself notes, ''the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.'' An SBOM advances transparency in the software supply chain, similar to a ''list of ingredients.'' NTIA is directed to publish a list of ''minimum elements for an SBOM.''

NTIA has played a leadership role in advocating for SBOM, convening experts from across the software world and leading discussions around the ideas of software supply chain transparency.[2] The goal of this Request for Comments is to seek input and feedback on NTIA's approach to developing and publishing the minimum elements of an SBOM. NTIA is committed to being open to further additions, corrections, deletions, or other changes, particularly when suggestions are well supported with

[1] Exec. Order No. 14,028 of May 12, 2021, 86 FR 26,633 (May 17, 2021).

[2] See David J. Redl, NTIA Launches Initiative to Improve Software Component Transparency, Nat'l Telecomm. & Info. Admin. (June 6, 2018), *https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency;* Allan Friedman, Dir., Cybersecurity, Nat'l Telecomm. & Info. Admin., Transparency in the Software Supply Chain: Making SBOM a Reality, Address at Black Hat USA 2019 Conference (Aug. 7, 2019).

documents, operational evidence, and support from broad-based constituencies in the software ecosystem.

Since 2018, NTIA has coordinated an open and transparent multistakeholder process on software component transparency, providing a forum in which a diverse and evolving set of experts and interested parties have been able to weigh in, share their leadership and respective visions, unpack the complex challenges of software supply chain, and propose various solutions.[3] The idea of an SBOM is not new. Its roots lie in the concepts developed by noted American engineer and management consultant W. Edward Deming to build post-war industrial supply chain leadership, and over the last decade an SBOM has come to be considered vital to security by notable security experts.[4] By providing a forum for SBOM discussions, NTIA has helped the community identify common themes, coalesce around standards, and emphasize interoperability. These discussions have led to the documentation of existing tools, products, and projects, and have helped drive further experimentation and implementation. With an emphasis on the practice of SBOM generation and use, NTIA has sought to facilitate ''proof-of-concept'' exercises in specific communities and sectors.[5] NTIA has also worked across the federal government to share ideas about SBOM, seek feedback and engagement from experts in the civilian and national security community, and expand general awareness of SBOM.

What is an SBOM?

The Executive Order defines an SBOM as ''a formal record containing the details and supply chain relationships of various components used in building software.'' It refers to what the software assurance organization SAFECode calls ''third party components.'' Software is made and used by a wide range of organizations, but this diversity makes a single model for SBOM difficult. There is no one-size-fits-all approach to providing transparency for software assurance.

The Executive Order also defines SBOM in functional terms, framing its value in terms of use cases. It notes distinct but overlapping benefits that accrue to the organization that makes the software (''developers''), the organization that chooses or buys software, and those that operate software. Many of these use case benefits center around tracking known or newly identified vulnerabilities, but SBOM can also support use cases around license management and software quality/efficiency, and can lay the foundation to detect software supply chain attacks. These benefits should serve as a lodestar for designing and publishing the minimum elements of an SBOM that can be applied across the diverse software ecosystem.

Potential Elements for an SBOM

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 for automation. Focusing on these three elements will enable an evolving approach to software transparency, and serve to ensure that subsequent efforts will incorporate more detail or technical advances. The information below is preliminary, and the ultimate list published by NTIA will be revised based on public input.

Data fields. To understand the third-party components that make up software, certain data about each of those components should be tracked. This ''baseline component information'' includes:[6]

- Supplier name
- Component name
- Version of the component
- Cryptograph hash of the component
- Any other unique identifier
- Dependency relationship
- Author of the SBOM data

Some of these data fields could be expanded. For example, the ''dependency relationship'' generally refers to the idea that one component is included in another component, but could be expanded to also include referencing standards, which tools were used, or how software was compiled or built. Other data fields may need more clarity, including data fields for component and supplier name. As one SBOM document notes, ''[c]omponent identification is fundamental to SBOM and needs to scale globally across diverse software ecosystems, sectors, and markets.''[7] The challenge is that different technical communities and organizations have different approaches to determining software identity.

Operational considerations. SBOM is more than a set of data fields. Elements of SBOM include a set of operational and business decisions and actions that establish the practice of requesting, generating, sharing, and consuming SBOMs. This includes:

- Frequency. Operational considerations touch on when and where the SBOM data is generated and tracked. SBOM data could be created and stored in the repository of the source. For built software, it can be tracked and assembled at the time of build. A new build or an update to the underlying source should, in turn, create a new SBOM.
- Depth. The ideal SBOM should track dependencies, dependencies of those dependencies, and so on down to the complete graph of the assembled software. Complete depth may not always be feasible, especially as SBOM practices are still novel in some communities. When an SBOM cannot convey the full set of transitive dependencies, it should explicitly acknowledge the ''known unknowns,'' so that the SBOM consumer can easily determine the difference between a component with no further dependencies and a component with unknown or partial dependencies.
- Delivery. SBOMs should be available in a timely fashion to those who need them and have proper access permissions and roles in place. Sharing SBOM data down the supply chain can be thought of as comprising two parts: How the existence and availability of the SBOM is made known (advertisement or discovery) and how the SBOM is retrieved by or transmitted to those who have the appropriate permissions (access).[8] Similar to other areas of software assurance, there will not be a one-size-fits-all approach. Anyone offering SBOMs must have some mechanism to deliver them, but this can ride on existing mechanisms. SBOM delivery can reflect the nature of the software as well: Executables that live on endpoints can store the SBOM data on disk with the compiled code, whereas embedded systems or online

[3] NTIA, Multistakeholder Process on Promoting Software Component Transparency, Notice of Open Meeting, 83 FR 26,434 (June 7, 2018).

[4] See Seth Carmody et al., Building Resilient Medical Technology Supply Chains with a Software Bill of Materials, 4 npj Digit. Med., at 1, 1–2 (2021), *https://doi.org/10.1038/s41746-021-00403-w.*

[5] See Susan Miller, Protecting the Supply Chain with a Software Bill of Materials, GCN (Feb. 22, 2021), *https://gcn.com/articles/2021/02/22/sbom-supply-chain-security.aspx.*

[6] See generally Framing Working Grp., Nat'l Telecomm. & Info. Admin., Framing Software Component Transparency (2019), *https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf* (providing further information on baseline components).

[7] Framing Working Group, Nat'l Telecomm. & Info. Admin., Software Identification Challenges and Guidance (2021), *https://www.ntia.gov/files/ntia/publications/ntia_sbom_software_identity-2021mar30.pdf.*

[8] Framing Working Grp., Nat'l Telecomm. & Info. Admin., Sharing and Exchanging SBOMs (2021), *https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf.*

services can have pointers to SBOM data stored online.

Automation support. A key element for SBOM to scale across the software ecosystem, particularly across organizational boundaries, is support for automation, including automatic generation and machine-readability. As the Executive Order notes, SBOMs should be machine-readable and should allow ''for greater benefits through automation and tool integration.'' Manual entry or distribution with spreadsheets does not scale, especially across organizations.

The SBOM community has identified three existing data standards (formats) that can convey the data fields and be used to support the operations described above: SPDX,[9] CycloneDX,[10] and SWID tags.[11] Experts in these formats have mapped between them to create interoperability for the baseline described above. Because these formats already are subject to public input and translation tools exist, they serve as logical starting points for sharing basic data.[12]

In addition to the three SBOM formats, the need for automation defines how some of the fields might be implemented better. For instance, machine-scale detection of vulnerabilities requires mapping component identity fields to existing vulnerability databases.

Request for Comment

The discussion above lays out the collected data points and experience from experts and practitioners in SBOM, including existing practices and novel proof-of-concept work. To inform, validate, and update NTIA's understanding of SBOM, NTIA seeks comment on the following questions:

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

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

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.

a. 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.

b. 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 that is not running on customer premises or maintained by the customer.

c. 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.

d. 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.

e. 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 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?

f. 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?

g. 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.

h. 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.

i. 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.

j. 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.

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?

Instructions for Commenters: NTIA invites comment on the full range of issues that may be presented in this Notice, including issues that are not specifically raised in the above questions. Commenters are encouraged to address any or all of the above questions. Comments that contain references to studies, research, and other empirical data that are not widely available should include copies of the referenced materials with the submitted comments. Comments submitted by email should be machine-readable and should not be copy-protected. Responders should include the name of the person or organization filing the comment, which will facilitate agency follow up for clarifications as necessary, as well as a page number on each page of their submissions. All comments received are a part of the public record and will be posted on *regulations.gov*

[9] See also SPDX, *https://spdx.dev/* (last visited May 18, 2021).

[10] See also CycloneDX, *https://cyclonedx.org/* (last visited May 18, 2021).

[11] See David Waltermire et al., Guidelines for the Creation of Interoperable Software Identification (SWID) Tags (2016) (Nat'l Inst. of Standards & Tech. Internal Rep. 8060), *http://dx.doi.org/10.6028/NIST.IR.8060* (SWID tags are defined by ISO/IEC 19770–2:2015).

[12] See, *e.g.,* SwiftBOM—SBOM Generator for PoC and Demos, *https://democert.org/sbom/* (last visited May 18, 2021).

[13] Exec. Order No.14028 § 4(e)(i)–(x), 86 FR 26633, 26638–39 (May 12, 2021).

[14] David Braue, Software 'Bill of Materials' To Become Standard?, Info. Age (Oct. 22, 2020, 11:34 a.m.), *https://ia.acs.org.au/article/2020/software-bill-of-materials-to-become-standard.html.*

and the NTIA website, *https://www.ntia.gov/,* without change. All personal identifying information (for example, name, address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information.

Dated: May 27, 2021.

Kathy D. Smith,

Chief Counsel, National Telecommunications and Information Administration.

[FR Doc. 2021–11592 Filed 6–1–21; 8:45 am]

BILLING CODE 3510–60–P

DEPARTMENT OF COMMERCE

Patent and Trademark Office

[Docket No.: PTO–P–2021–0010]

Submitting Patent Applications in Structured Text Format and Reliance on the Text Version as the Source or Evidentiary Copy

AGENCY: United States Patent and Trademark Office, Department of Commerce.

ACTION: Notice.

SUMMARY: The United States Patent and Trademark Office (USPTO) is in the process of transitioning to a system that supports submitting new patent applications in structured text, specifically DOCX format. Filing in structured text allows applicants to submit their specifications, claims, and abstracts in text-based format, thereby eliminating the need for applicants to convert applications into a PDF for filing. It also provides a flexible format with no template constraints and improves data quality by supporting original formats for chemical formulas, mathematical equations, and tables. The USPTO previously stated that for applications filed in DOCX, the authoritative document would be the accompanying PDF that the USPTO systems generate from the DOCX document. In response to public feedback, however, the USPTO now considers the DOCX document filed by the applicant to be the authoritative document. Accordingly, an applicant who files or has filed an application in DOCX may rely on that version as the source or evidentiary copy of the application to make any corrections to the documents in the application file. The USPTO will be hosting DOCX training sessions to provide more information, demonstrate how to file and retrieve DOCX files in Patent Center, EFS–Web, and PAIR, and answer any questions. Applicants can also file test submissions through Patent Center training mode to practice filing in DOCX. In addition, we will be offering listening sessions to gather feedback and suggestions to further improve DOCX features.

DATES: *Effective date:* June 2, 2021.

FOR FURTHER INFORMATION CONTACT: Mark O. Polutta, Senior Legal Advisor, 571–272–7709, or Eugenia A. Jones, Senior Legal Advisor, 571–272–7727, of the Office of Patent Legal Administration, Office of the Deputy Commissioner for Patents.

For technical questions related to submitting documents in DOCX format, please contact the Patent Electronic Business Center (EBC) at 1–866–217–9197 (toll-free), 571–272–4100 (local), or *ebc@uspto.gov*. The EBC is open from 6 a.m. to midnight, ET, Monday through Friday.

SUPPLEMENTARY INFORMATION: The USPTO is in the process of transitioning to a system that supports submitting new patent applications in structured text, specifically DOCX format. Application documents submitted in DOCX format will facilitate the examination and publication processes. This notice provides information on structured text filing. Specifically, the USPTO now considers the DOCX documents filed by applicants to be the authoritative document, otherwise referred to as the source or evidentiary copy of the application, for purposes of determining the content of the application as originally filed, should a discrepancy be discovered. This notice does not require patent applicants to make any changes to their practices.

Currently, applicants may electronically file an application either by submitting PDF files or by submitting DOCX files. If an applicant submits DOCX files, the USPTO uses the DOCX files to generate PDF files prior to the actual filing of the application. The USPTO published a final rule on setting and adjusting patent fees on August 3, 2020. *See* Setting and Adjusting Patent Fees During Fiscal Year 2020, 85 FR 46932 (Aug. 3, 2020). In addition to establishing a fee for applications not submitted in a DOCX format, the response to comment 54 in the final rule stated that for applications filed in DOCX, the authoritative document will be the accompanying PDF that the USPTO systems generate from the DOCX document. *See id.* at 46957.

In response to public feedback, the USPTO has changed what will be the authoritative document. The USPTO is informing applicants that it now considers the DOCX documents filed by applicants to be the authoritative document, otherwise referred to as the source or evidentiary copy of the application. This change applies to all patent documents submitted in DOCX format, including DOCX submissions made prior to this notice.

The source or evidentiary copy of the application is the version submitted to the USPTO by the applicant in one of the following formats: Paper, DOCX, or PDF when not accompanied by a DOCX version of the same. Applicants should not submit PDF versions they created when filing an application in DOCX, as they are unnecessary. If the applicant submits documents in DOCX along with PDF versions they created (not the auto-generated PDFs created by the USPTO), then the DOCX version will still be considered the source or evidentiary copy, and the applicant will be required to pay the non-DOCX surcharge fee.

Applicants can rely on the DOCX version as the source or evidentiary copy in order to make any corrections to the record when any discrepancies are identified between the source or evidentiary copy and the documents as converted by the USPTO. Accordingly, during the filing process, applicants will be advised to review the DOCX files before submission rather than reviewing the USPTO-generated PDF version, as set forth in the August 3, 2020, final rule.

However, applicants are advised to check the USPTO-generated versions as soon as practicable for any discrepancies or errors. Any discrepancies or errors that occur as a result of filing an application in DOCX format should be promptly brought to the attention of the USPTO. Applicants should initially contact the Patent EBC for investigation at 1–866–217–9197 (toll-free), 571–272–4100 (local), or *ebc@uspto.gov*. Depending on the situation, applicants may need to file a petition under 37 CFR 1.181 in order to have the issue reviewed and addressed. This is consistent with current USPTO procedures for documents filed in patent applications.

In this regard, the USPTO has a records retention schedule for documents it receives, including new patent applications and correspondence filed in patent applications. For example, applications filed in paper via mail or hand-delivery are scanned into the image file wrapper (IFW) or the Supplemental Complex Repository for Examiners (SCORE), as appropriate. In 2011, the USPTO established a one-year retention policy for patent-related papers scanned into the IFW or SCORE. *See* Establishment of a One-Year Retention Period for Patent-Related Papers That Have Been Scanned Into the