UNITED STATES OF AMERICA
BEFORE THE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Request for Comment (RFC) on Software Bill of	**)**
Materials Elements and Considerations	**)**
NTIA-2021-0001	**)**

VIA EMAIL
SBOM_RFC@ntia.gov

COMMENTS OF FORTRESS INFORMATION SECURITY AND ITS SUBSIDIARY CYBER RISK UTILITY, LLC D/B/A ASSET TO VENDOR NETWORK ("A2V")

1. ABOUT RESPONDENT

Fortress Information Security, together with its subsidiary Cyber Risk Utility, LLC (d/b/a the "Asset to Vendor Network or "A2V" or "Fortress") provides cyber supply chain risk management solutions, and our mission is to secure critical infrastructure by managing cyber supply chain risks from vendors to assets. Fortress specializes in Utilities, the Department of Defense, the Department of Homeland Security, and their critical suppliers.

This remainder of this section is referred to as "Our Solutions" or "Cyber Supply Chain Risk Management Solutions ("C-SCRM")."

In pursuit of our mission, Fortress delivers four capabilities: (1) proprietary software known as the Fortress Platform, (2) an information sharing exchange known as A2V, (3) vendor and product risk tools, data, and analytics such as software bill of materials (SBOM) analysis, hardware bill of materials (HBOM) analysis, product security assessments, the Related Entity Discovery methodology ("RED") and File Integrity Assurance ("FIA"), and (4) a variety of

managed services to help our clients produce results. The Fortress Platform enables cyber supply chain risk management program execution and maturity. The A2V information sharing network is the only central repository focused exclusively on the unique needs of the Utility Industry and its critical suppliers. Finally, Fortress correlates dozens of data sources and its cadre of research analysts and engineers conduct comprehensive monitoring and data-driven solutions, which cover cybersecurity, FOCI, components, and other risks.

2. RESPONDENT'S EXPERIENCE

This section is collectively known as "Our Work" or "Fortress' Experience."

Fortress provides Cyber Supply Chain Risk Management Solutions to investor-owned utilities ("IOUs"), regional transmission organizations ("RTOs"), Public Utilities, Utility Cooperatives, and their critical suppliers.[1] In total, it is our privilege to serve over 100 energy companies, subsidiaries and their critical suppliers, employing over 250,000 employees (about half the population of Wyoming), providing energy to over 50 million people (about twice the population of Texas) in the lower 48 states. We manage the cyber risk on over 40,000 vendors and 1,000,000 assets for our clients. We established the A2V network in partnership with American Electric Power ("AEP") and Southern Company ("Southern").[2] The A2V network is a central repository used by our clients and over a hundred of their most critical suppliers driving security and trust through transparency. AEP, Southern and Fortress understand the prohibitive cost of cyber securing the supply chain, and so, A2V has been patterned after the success in the financial industry to drive maturity and reduce compliance costs. It is estimated that A2V can

[1] We also provide cyber supply chain risk management solutions to the DOD and DHS.
[2] ASSET TO VENDOR, https://assettovendor.com/ (last visited June 7, 2021).

save the industry $8 billion (about $25 per person in the US) in compliance costs in the first five years excluding the business benefits and risk reduction.[3]

We operationalize clients' compliance with the North American Electric Reliability Corporation's ("NERC") Critical Infrastructure Protection ("CIP") reliability standards.[4] We also operationalize our clients' cyber supply chain security programs using recognized frameworks, such as that of National Institute of Standards and Technology ("NIST") for Improving Critical Infrastructure Cybersecurity.

At Fortress, we see different maturity levels in our clients' (both asset owners and their critical suppliers) cyber supply chain programs. The A2V network drives maturity by easing expertise and financial constraints on less resourced asset owners and suppliers. Instead of each utility company completing its own supply chain risk assessment, we complete the risk assessment and share congruent information to simplify what otherwise would be a redundant, costly, and burdensome process for asset owners and their suppliers. Thus, a central repository like A2V increases cyber supply chain maturity by sharing information, driving best practices, and reducing compliance costs to all those involved, particularly less resourced asset owners, suppliers, and other stakeholders such as State and local governments and Indian Tribes.

The industry's central repository, A2V, that Fortress operates, contains information on 20,000 vendors and products. We monitor these vendors' and products' bills of materials, security controls, vulnerabilities, FOCI, and breaches. We have completed tens of thousands of assessments of vendors and products just in the last year. These assessment include validated

[3] Fortress supplied detailed calculations of these savings as part of its response to the Department's RFI in September 2020.
[4] See, e.g., North American Elec. Reliability Corp. [NERC], Cyber Security – Supply Chain Risk Management, CIP-013-1, (2021), https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

vendor control assessments, any-source vendor assessments, any-source product assessments, product teardowns, software Bill of Materials ("SBOM") assessments, hardware Bill of Materials ("HBOM") assessments, FOCI assessments ("RED"), and File Integrity Assessments ("FIA").

The first step to long-term successful cybersecurity requires full C-SCRM program maturity and resources to achieve the requisite maturity. Our Work has taught us that while asset owners and their suppliers have expended tremendous effort and resources to implement C-SCRM programs, many as recently as the last year, much more maturation needs to take place to cyber secure our supply chain. There is little time as the threat is upon us.[5] Collaboration and support between the private sector and governmentat all levels, the utility industry, and the cybersecurity industry, will facilitate achieving full maturity, and subsequently, successful cybersecurity. We accelerate achieving C-SCRM program maturity by removing duplicative, inefficient work on behalf of every industry participant involved.

3. OPENING COMMENTS

Fortress believes we are at a critical juncture in the defense of our nation's infrastructure, and the need for software transparency and software bill of materials (SBOM) has become quite apparent in the wake of such attacks such as Solarwinds and recent new techniques such as Dependency Confusion[6]. We applaud the current administration in making SBOM a priority in

[5] See, e.g., SOLARWINDS, https://www.solarwinds.com/sa-overview/securityadvisory (last updated Apr. 6, 2021, 9:00 AM)
[6] Dependency Confusion, https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610 (last updated Feb. 9, 2021)

Executive Order 14208[7] and are encouraged that policymaking on the national stage is in alignment with Fortress existing strategies to secure these critical supply chains.

Further, we believe that the proposed initiatives are a reasonable starting point, but represent the beginning of a journey, and not the ultimate destination for securing software supply chains. To that end, the comments contained within this RFC encapsulate our belief that SBOM alone, while crucial as a starting point, requires additional risk context to produce the desired results. We also believe that a management and sharing infrastructure such as the Fortress A2V model and the risk orchestration provided by a platform such as Fortress Platform, is required to facilitate this ecosystem and drive value for SBOM related activities.

4. INFORMATION REQUESTED

In this Request for Comment ("RFC") by the Department of Commerce through the National Telecommunications and Information Administration ("Department" or "NTIA"), has proposed the following baseline set of data fields for inclusion into a SBOM:

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

[7] Executive Order 14208 on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (last updated May 12, 2021)

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?

Fortress opines that the above data fields represents a defensible minimum number of fields to include in a SBOM in order to gain supplier adherence to this practice. It is important to note that file hashes should be constructed using currently defensible mechanisms such as SHA-256. MD5 should not be used due to cryptographic weaknesses. There are a number of other data fields listed below that Fortress believes are important to consider, but not at the risk of endangering supplier cooperation:

- Document metadata fields to include:
    - Unique SBOM document name
    - SBOM document format and version
    - Where SBOM is supplied such as the unique URL it can be retrieved from
    - SBOM creation date
    - SBOM modification date
    - SBOM revision number
    - Document digital signature/code signing
    - Registered publisher name for the digital signature for the document
- Product metadata fields to include:
    - Unique product identifier to include model number, revision, etc.
    - Product supplier

    - Product type (hardware, software, etc)
    - Product category (networking, database, SCADA, etc)
    - Product function (
    - Document digital signature/code signing
    - Registered publisher name for the digital signature for the software product
    - Alternate publisher name if code signing is performed by a different entity than software publisher

- Device relationships – a product is a sum of its parts including software and hardware. The relationships between hardware and software is crucial when determining the importance of a component
- Additional hardware bill of materials (HBOM) information. While we note that HBOM is out of scope for NTIA efforts, Fortress believes that a singular SBOM document, can and should contain the entirety of the ingredients for the product, including hardware. Fortress maintains an additional list of required HBOM fields we can supply in future documents.
- Component sourcing such as whether it is contained within the software project itself, retrieved from a repository such as NPM, or expected to be provided such as a system library.
- Whether the components are "private" to the software project or publicly obtainable. For instance an NPM repository can be public or private only inside suppliers environment.

- Third party components unique URL for the authoritative source for the package. Open source software is frequently difficult to understand if it is built from a forked version or not.
- Component creation and update timestamps
- Component changes from one version to the next, including what has changed

Additionally, we believe that dynamic changes to software such as identified vulnerabilities, and changes to software support status should be captured in a URL defined in the SBOM document where the software consumer can update information without needing a new SBOM to be generated. For instance, the software may not change, but if the software is sunset and is no longer supported, it would be desirable to know this. However, as the software is unchanged, it is inappropriate to generate a new SBOM document until there is an actual code level change, or a revision to a required SBOM data element. Vulnerabilities will be discussed in the section 3 below.

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

The primary use case we have identified that is not captured in Section 3 below, is that of foreign adversarial control and influence, or FOCI. This is a difficult problem to solve for, especially for open source software. This does not mean that it is impossible or unsolveable, and Fortress maintains FOCI is an important risk consideration for our nation's interests. A secondary, but related, use case involves the understanding of where banned suppliers exist in the software. In most cases these are hardware component restrictions such as those found in the National defense Authorization Act, however software suppliers like Kaspersky are banned, and

until recently many Chinese payment providers were banned under prior executive orders. This remains a topic of policy-making, and the need to understand where software comes from is very petinent to these regulatory requirements.

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.

The topic of naming is a core concern for SBOM, largely due to how software is named internally within a software project as opposed to how software is named externally and referenced by the community. The practice of common platform enumeration, or CPE[8], is applied inconsistently, and while it is better than no standards, variations in conformance creates many challenges, as does the fact that most open source components never receive a CPE designation. Until a better solution is proposed, Fortress encourages the adoption of CPE as a standard mechanism, and suggests that NIST work with industry to create a mapping reference for software components to CPE. This could conceivably become similar to how domain name services (DNS) resolution revolutionized the internet. We hear NTIA had something to do with that.

[8] Common Platform Enumeration. https://nvd.nist.gov/products/cpe (Retrieved June 16, 2021)

CPE has also been established as the primary mechanism for identifying vulnerabilities in the National Vulnerability Database, and as such we do not suggest abandoning this mechanism. This is arguably the most important use case we will discuss in this document.

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.

Fortress does not believe that software as a service is fundamentally different than any other software, except for the lack of transparency in SaaS software and increased complexity of infrastructure. Additional differences include the fact that there are frequently external services utilized, but cloud infrastructure and external services and dependencies should be described in SBOMs in much the same way as on-platform software products. All users of software deserve software transparency, regardless if they are an operator of the software installation.

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.

We agree that legacy products produce significant challenges, largely due to the lack of automation capabilities as these products utilize older build methods, or in some cases, utilize legacy binaries where source code is not known or well-understood. For this reason, we believe that the tool solution space requires capabilities for binary based SBOM creation when source code based, or build environment based solutions are not feasible. While these approaches typically have lower confidence than traditional source composition analysis (SCA) based

approaches, the large number of legacy products in use, especially in critical infrastructure, requires that these considerations be made. To put it simply, SCA tools today are not sufficient to meet this need as most of them require software manifest files, or access to source code.

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.

Fortress has long focused on software integrity and authenticity as a key use case, especially with our alignment with NERC CIP standards that also require this level of analysis. For this reason, we feel that hashing and code signing are very useful mechanisms to illuminate these risks. We believe the NTIA guidance is largely supportive of this use case, but would like to see stronger cryptographic techniques such as code signing, and documented best practices for how to properly manage code signing in a high trust fashion to allow for greater assurance. Use of trusted 3rd party certificate authorities instead of self-signed code would be ideal, but in some cases it is not necessary such as applications where internet usage is unlikely and 3rd party certs cannot be validated.

Additionally, we believe that stronger code check-in processes within the development pipeline can greatly strengthen this approach. For instance, requiring two separate developers to authorize the code commit, or performing integrity based validation inside the source repository can be very effective mechanisms. We believe that these security attestations and activities could easily be included within an SBOM to signify the good security practices employed by software developers, or the lack thereof can serve as a canary to indicate when weak practices are likely

occurring. Such records should be cryptographically signed and timestamped to provide further assurance that they occurred as indicated.

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?

See **section d.** Furthermore, Fortress proposes that management of software components within a software project such as automated deployment from code repositories is a critical threat vector that cannot be understated.

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. How can SBOM data be integrated with this additional data in a modular fashion?

While Fortress is hard at work on this particular use case, we are not prepared with a comment at this time. See **section d.** for our comments on security attestation within the SBOM.

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.

Fortress proposes to industry to deliver a shared ecosystem for the facilitation of risk information sharing. As such, we are highly interested in the concept of an SBOM exchange, in much the same way as we facilitate information sharing between asset owners and suppliers today within the A2V risk assessment and attestation sharing infrastructure. We recognize that there is a large gulf between stakeholders, and that use cases may vary dramatically from one consumer to another, from one risk profile to another, and management of this ecosystem is critical to ensure that oversharing or data integrity issues do not arise, creating unintended risk consequences.

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.

Fortress agrees that while depth is desired, it should not be required for every SBOM, unless the assurance needs for the product are high. We support the efforts of the OWASP software component verification standard (SCVS)[9] that applies a risk-based approach for software supply chain verification activities. This provides for an acceptable baseline for all software, while increasing the rigor for software with higher assurance requirements. Some of the optional data fields we have proposed could easily fit within a model such as this, and when combined with the definition of critical software, as well as consumer safety labeling for software, provides a mechanism to attest to the security of software in a measured way.

[9] Software Component Verification Standard, https://owasp.org/www-project-software-component-verification-standard/ (Retrieved June 17, 2021)

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.

Fortress opines that SBOMs are best suited for static data that will not change until the software itself changes. As such, vulnerability is best suited for external documents such as a VEX, or Vulnerability Exploitability Exchange. By uniquely naming software components in an SBOM, a vulnerability management system can identify many potential vulnerabilities through CPE correlation to the NVD. These vulnerabilities will likely have an extremely high false positive rate until they can be validated. This is due to the scenario where 3rd party components are included in code, but not called, or the vulnerable functions are not used, or user input cannot influence the vulnerable function, or many other similar reasons. While this information is very useful, due to the uncertainty of information and rapidly changing nature of security research, this data should be referenceable by a supplier provided URL where up to date information can be retrieved, or SBOMs could be enriched with 3rd party sources of VEX data used for this purpose.

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’’), but other solutions may exist.

Fortress manages supply chain risk through our proprietary software platform, known as the Fortress Platform. By leveraging the power of data aggregation and advanced analytics at machine speed, and a big data fplatform to correlate massive data sets, a truly continuous risk delivery model begins to emerge that dovetails very well with emerging risk insights such as those provided by SBOM. Even moreso, when software security insights are contextualized against real asset lists and further classified through impact and consequences based drivers, risk management starts making a lot more sense.

The crux of the larger problem facing the SBOM community, is what happens after we get the suppliers to agree to providing SBOM? What do we do with all these XML and JSON documents? How can asset owners consume this content on a continuous basis and make this information actionable? What are the appropriate actions that SBOM consumers should be taking? They certainly can’t patch every vulnerability but perhaps leveraging this information to apply pressure to software suppliers makes sense. That has certainly been our experience, and why we are proud to stand behind our platform to continuously consume, transform and ultimately share risk insights through the A2V marketplace described within this document and provide tools for software users to manage and mitigate software risks.

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?

Adoption of SBOM is non-negotiable. This should be the minimum bar for suppliers to adhere to, and far too low to ensure their good stewardship of software we rely on every day to feed and sustain our way of life. An SBOM is nothing more than an inventory of software and their components. Inventory is a foundational concept in risk management, as without know what you need to protect, it is nigh impossible to secure it.

There are also many other excellent software security practices provided by OWASP, NIST and others that can support proactive security controls, software assurance and governance, security testing and many other similar activities. At the root of all of these practices, is the fundamentl need to understand what is being protected, and a set of security objectives that inform us of our priorities to achieve an acceptable level of risk.

5. CLOSING COMMENTS

The energy sector is a key stakeholder in America's cleaner sustainable future.[10] To enable this future, the energy industry is leading a digital transformation and an electrification of our economy. This progress, however, comes with considerable cyber risk that our adversaries are clearly intending to exploit. It is therefore essential that the United States strengthen its critical infrastructure cyber defenses including that of its vast supply chain. This must be done as quickly as possible. The good news is that the private utility industry, comprised of asset owners and their suppliers, as supported by government at all

[10] Molly Whalton, If the Energy Sector Is to Tackle Climate Change, It Must Also Think About Water, International Energy Agency (Mar. 23, 2020), https://www.iea.org/commentaries/if-the-energy-sector-is-to-tackle-climate-change-it-must-also-think-about-water.

levels are building and maturing supply chain cyber security programs. Recent attacks highlight that more needs to be done and faster.

Our Solutions help utilities identify and manage IT and OT Bulk Electric Systems ("BES") including software patches and configurations for those systems. Fortress' Experience is that utilities can identify critical infrastructure within their service areas that either they or regulations have identified high-risk. However, Our Work around the NDAA Section 889 requirement's, EOs and CIP standards also show that identifying hardware and software components (i.e., HBOM and SBOM) is a new and challenging requirement that necessitates cooperation between asset owners and suppliers, especially considering our objective to accelerate cyber supply chain maturity. As previously written, a public-private partnership together with standardization and utilization of a central repository will accelerate maturity in this area and enhance access to these resources to smaller asset owners and suppliers.

Based on Our Work providing C-SCRM Solutions to asset owners and critical suppliers, we observe that the sophistication of cyber supply chain security programs is inconsistent, and therefore, some programs are more effective than others. This is a predictable outcome considering the scarcity of cyber security talent and disparity of resources between large and small entities. To mitigate this, we recommend:

> (1) continued adoption of the SBOM requirements in EO 14208,
> (2) Further maturation of the software supply chain best practices by (i) adopting standards such as those published by the Open Web Application Security Project, National Institute of Standards and Technology, North American Transmission Forum and the Idaho National Laboratory and (ii) utilizing an operational central repository such as A2V to avoid waste and duplication and enable reallocation of scarce resources to higher effectiveness activities, and
> (3) providing less resourced asset owners and suppliers financial assistance to secure themselves.

As citizens and stakeholders, we must work together to cyber secure our nations and planet's future.