June 17, 2021

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

**SUBJ: Notice and Request for Comments on Software Bill of Materials Elements and Considerations (NTIA-2021-0001)**

Dear Ms. Remaley:

On behalf of the Aerospace Industries Association of America (AIA), I am pleased to offer the enclosed comments in response to the request for comments on the minimum elements for a Software Bill of Materials (SBOM), and what other factors should be considered in the request, production, distribution, and consumption of SBOMs. For over 100 years, AIA has been the industry voice shaping the policies that matter most to our members, comprising over 320 of the nation’s leading aerospace and defense manufacturers and suppliers of civil, military, and business aircraft, helicopters, unmanned aerial systems, space systems, aircraft engines, missiles, materiel, and related components, equipment, services, and information technology. AIA and its member companies appreciate NTIA’s consideration of our comments as the Department of Commerce achieves the milestones per President Biden’s Executive Order on Improving the Nation’s Cybersecurity.

AIA member companies support the Department of Defense across a variety of Development, Security, & Operations (DevSecOps) activities in support of national security programs. Success has been achieved thru DoD’s criteria for Software Factories (SWF) to include key cybersecurity requirements directing missions operating on timelines of hours, days, and weeks, not months and years. Software must be transformed from using the long lead ‘waterfall’ development framework to an iterative and incremental DevSecOps methodology delivering the most critical features first. The automatic generation of SBOM data is a key element of the SWF premise and inherently indictive for dynamic environments. We support the Open Web Application Security Project (OWASP) CycloneDX standard for SBOM generation, which partially aligns to NTIA’s currently published fifteen “minimum elements of an SBOM”. While the CycloneDX standard supports these “minimum elements of an SBOM,” all elements are not guaranteed to be present, depending on the source material. Various tools, programs, and services can be leveraged for the generation and manipulation of SBOM data.

The following three recommendations with accompanying suggestions offer critical topic discussions regarding the questions published on general SBOM practices:

1. The topics illustrate the broad scope of the digital domain whereas the cornerstones should be prioritized foremost to include assurance elements while also accounting for risk management and threat modeling.

- With the limited timeframe of ~10 business days, as opposed to the standard 60-day comment period, our detailed reviews and inputs on the supplementary request related to the complex questions on elements, use cases, & operational requirements are constrained.
- We strongly advise against including a Vulnerability List in the data fields specifically, as a vulnerability list is the product of one or more vulnerability analysis efforts, not an SBOM. The ability to exchange with a standard format for currently associated vulnerabilities against the SBOM is advisable, though the analysis and reporting of such concerns may be held in a separate location. Existence and status of vulnerabilities can change over time, with no guarantee or signal on whether the SBOM data is up to date.

2. Value Stream Mapping is an essential practice that should be used to demonstrate actionable capabilities, value in operations, and allocation of resources over static informative specifications.

- Expanding the NTIA SBOM minimal elements to include NIST software assurance activities, lessons learned and mitigations from previous experiences related to incidents to include damage assessments is critical to the overall software and cyber landscape.
- We recommend processes to support the objective use cases of vulnerability/weakness analysis, vulnerability and incident response, supply chain assessment, pedigree and integrity of the software product, and dependent elements to include SBOM confidentiality and integrity.
- We also assert that automation tools built within DevSecOps SWFs can be used to generate supporting artifacts to accommodate frequent (e.g., daily) vulnerability status changes to part, or all, of a package and associated SBOM.

3. Software Engineering recognized processes, international standards, and related innovative concepts should be reviewed, analyzed, and considered before authoring U.S.-only standards.

- Since the digital scope is dynamic and not U.S.-specific, a digital bill of materials must function in international markets with operational assurances that extend across sectors. As an example, in Aviation, extra properties may need to be added for Software Assurance Level (SAL), Design Assurance Level (DAL), or Item Development Assurance Level (IDAL).
- We recommend a lightweight SBOM specification, capable of achieving real-world use cases across vendors or suppliers. CycloneDX, as an example, is a recognized risk-based open source project developing the specification, implementations, and providing standards in XML, JSON, and Protocol Buffers, as well as a large collection of official and community supported tools that create or interoperate across financial services, manufacturing, government, software, and security firms.
- Modular open systems architecture is key in supporting assorted technologies such as Kubernetes container orchestration that drives modularity through containerized microservice architecture into deployed systems. Modular approaches can simplify testing and deployment while enabling a hardware agnostic software solution across cloud providers that extends into embedded environments.

We are committed to initiatives that secure information from the advanced persistent threat (APT) as evidenced by our public comments to numerous proposed cyber-related requirements applicable to contractors and subcontractors' nonfederal information systems. By coordinating lessons learned with the supply chain thru the Defense Industrial Base (DIB) Sector Coordinating Council (SCC), we have demonstrated that requirements and processes in cybersecurity are mutually beneficial when shared through robust collaboration across government, industry, and sector business operations representing all U.S. and International stakeholders. To that end, we would gladly facilitate digitally focused working groups regarding our above comments with NTIA and our aerospace and defense industry partners.

Thank you for the opportunity to provide these comments. Should you have any questions, please contact me at jason.timm@aia-aerospace.org.

Sincerely,

Jason Timm
Director, Defense Policy & Integration