Business Software Alliance

Nick Andersen
Executive Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency

October 3, 2025

Executive Assistant Director Andersen:

Thank you for publishing the Request for Comment on the Cybersecurity and Infrastructure Security Agency (CISA) document 2025 Minimum Elements for a Software Bill of Materials. BSA continues to believe, and evidence continues to support, that public-private collaboration creates the strongest and most sustainable path to our shared version of a more secure future.

The Business Software Alliance (BSA) is the global trade association of the enterprise software industry, representing companies that are leaders in artificial intelligence, cybersecurity, cloud computing, quantum, and other breakthrough technologies. We work in over 20 markets in the US, Europe, and Asia, advocating for policies that build trust in technology so that every industry sector and the public can benefit from innovation.

BSA has long supported the development and use of SBOMs, recognizing their value as a tool for incident response. At the same time, we continue to caution against requiring SBOMs in procurement processes before stakeholders are equipped to ingest, interpret, and act on the information they contain.

BSA agrees with CISA that, as SBOM adoption expands across industries and borders, harmonizing expectations is critical. We strongly support CISA's efforts to ensure that both US Government agencies and international partners rely on a consistent definition of SBOM and require the same elements. Such harmonization not only simplifies and streamlines regulatory frameworks, but also strengthens security by, amongst other things: enabling clearer communication and collaboration among governments, agencies, and businesses; fostering a more robust marketplace for secure software; and reducing or eliminating unnecessary barriers to trade.

With regard to the 11 proposed data fields contained in the draft document, which are intended to "apply to software acquired or developed by agencies and the components of that software, including open-source software, artificial intelligence (AI) software, and software-as-a-service (SaaS)," BSA offers the following recommendations.

Component Hash

The sixth field, "component hash," would require an SBOM to include "The cryptographic value generated from taking the hash of the software component."

A hash can provide useful validation. However, two ambiguities must be addressed before it can be applied. First, it is unclear what exactly a software producer should provide a hash for. For example, is the

hash of a zipped archive of files or of the individual unzipped files? Second, for certain types of software, such as firmware, it is unclear whether a distinct "component" exists to be hashed at all.

The result is that, without further clarification, this requirement risks creating confusion and inconsistent implementation but providing a hash might still be helpful.

BSA recommends that CISA make component hash be a recommended field but not a required field.

License

The seventh field, "License," would require an SBOM to include "The license(s) under which the software component is made available."

The current draft may overly emphasize open-source licenses, but SBOMs must also capture commercial licensing information. Many enterprise software products include sublicensed or redistributed proprietary components, and clarity on both open-source and commercial licenses is essential.

BSA recommends that CISA balance and clarify its expectations for the license field.

Dependency Relationships

The eighth field, "Dependency Relationship," would require an SBOM to include "The relationship between two software components, specifically noting that Software X includes Component Y or that Component A is largely derived from Component B."

The dependency relationship is a valuable concept, but the description within the draft document conflates two related concepts. Dependency graphs illustrate which components depend on each other (e.g., Component A depends on Component B, which are each part of the primary component C). It is clear why this information is helpful. However, the draft also introduces ancestry and derivative information, which can also be helpful, but which is distinct.

Including two types of information (even if each on its own merits inclusion) in one field will decrease the value and usability of an SBOM.

BSA recommends CISA limit the field "Dependency Relationship" to dependency information and consider including derivative information in its own field.

Timestamp

The ninth field, "Timestamp," would require an SBOM to include a "Record of the date and time of the most recent update to the SBOM data" and more specifically use ISO 8601.

BSA supports the use of internationally recognized standards like ISO 8601. We note, however, that some SBOM formats rely on RFC 3339, a commonly used subset of ISO 8601.

BSA recommends CISA clarify that the timestamp field can use RFC 3339.

Practices and Processes: Known Unknowns

The subsection Known Unknowns in the section Practices and Processes would require an SBOM to explicitly identify known unknowns if it does not list all dependencies to create a distinction between software components with no further dependencies and software components for which the list of dependencies is incomplete. It also sets the default interpretation of an SBOM to be that it is incomplete.

Completeness

While the intent is to distinguish between components with no further dependencies and components for which the dependency list is incomplete, the framing creates confusion. By default, SBOMs are treated as incomplete, making the flagging of "unknowns" redundant. A clearer approach would be to require a machine-readable completeness declaration (e.g., complete / partial / unknown), with a defined scope. In addition, because redacted components are not "unknown" but intentionally withheld, the field should be renamed from "Known Unknowns" to "Completeness" to better reflect its purpose.

BSA recommends CISA rename the field "Completeness" and update the requirement accordingly.

External Dependencies in Open-Source Software

The draft document does not provide sufficient clarity for communicating external transitive dependencies in open-source software.

An SBOM author may not be able to achieve full transparency into external transitive dependencies in open-source and therefore cannot always provide complete information. For example, a software producer may use a pre-compiled library with its own internal dependencies that are not visible to the software producer. In such cases, full transparency cannot be expected, but the gap in information should be clearly communicated.

BSA recommends that CISA update the document to account for transitive dependencies in open-source software and allow SBOM authors to indicate when completeness cannot be assured.

* * *

BSA appreciates CISA seeking comments on its draft document and continues to be committed to working with CISA to make the digital ecosystem more secure and resilient, including through developing standardized SBOMs that users can operationalize to achieve concrete cybersecurity improvement.

Henry Young
Senior Director, Policy