Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

TO: **Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)**

RE: **RFC on Draft Guidance "2025 Minimum Elements for a Software Bill of Materials (SBOM)" – Docket No. CISA-2025-0007**

The Financial Sector Coordinating Council (FSSCC) appreciates the opportunity to comment on the draft "2025 Minimum Elements for a Software Bill of Materials (SBOM)" guidance that appeared in the Federal Register on August 22. The FSSCC is an industry-led, nonprofit established in 2002 to coordinate critical infrastructure protection across the financial services industry. Our membership includes financial institutions of all types and sizes, from community banks and credit unions to insurance companies, financial utilities and trade associations, representing the breadth of the sector.

We commend CISA's leadership in advancing software supply chain transparency. A SBOM provides critical context to software by detailing its constituent components, including open-source libraries, proprietary modules, and dependencies. This enhanced visibility is essential for bolstering both security and resiliency, as it enables proactive risk management, faster incident response, and greater supply chain accountability.

SBOMs play a vital role in enhancing software security. However, their effectiveness relies on establishing requirements that are practical, scalable, and harmonized with widely accepted schemas for documenting components and key software attributes, such as SPDX (Software Package Data Exchange) and CycloneDX (Cyclone Data Exchange).

Feedback on Currently Defined Elements

The strength of SBOM guidance lies in balancing what is feasible for producers with what is most useful for consumers. While many proposed fields add real value, others risk introducing complexity without advancing security outcomes.

Dependency Relationships: While these can provide value in specific contexts, including by informing understanding of lineage dependencies, in practice they often produce incomplete or inconsistent mappings. This may obscure rather than clarify risk. Improvements could support the development of dependency graphs and clarify component origin, but as currently defined, its utility is constrained.
Recommendation: Designate as optional rather than required until their value is demonstrated in practice.

Tool Name: Capturing the SBOM generation tool provides limited security value given inconsistencies in naming conventions and the prevalence of proprietary or custom-built solutions. Unless directly linked to validation or assurance functions, this field does not provide meaningful benefit.
Recommendation: Designate as optional rather than required until their value is demonstrated in practice.

Component Hash: We strongly support the inclusion of a component hash, the cryptographic value generated from taking the hash of the software component, as a minimum element. Clear guidance around cryptographic hash production and binary generation is essential to enable effective use. To maximize its utility, the guidance should clarify that the hash is valid only for the specific software version from which it was generated.

Recommendation: Refine the element description to specify both the algorithm used and the version of the software corresponding to the hash.

Feedback on Missing Elements

Several attributes are absent from the draft but are essential to being added into the guidance as minimum elements for clarity and effective risk management.

Component Manufacturer / SBOM Manufacturer: Distinguishing between the entity that built a component and the entity or tool that generated the SBOM is critical for accountability and transparency. Both should be required fields to ensure consumers have the necessary context regarding third-party involvement.
Recommendation: Add Component Manufacturer and SBOM manufacturer as minimum elements.

Component Type: Identifying whether a component is a library, application module, or firmware is essential for effective risk prioritization and remediation planning.
Recommendation: Add Component Type as a minimum element.

Known Unknowns: Both SPDX and CycloneDX allow for structured representation of incomplete data. Including this field will enhance transparency and enable consumers to appropriately manage cases where data is not fully complete.
Recommendation: Add Known Unknowns as a minimum element.

Additional Feedback

We believe it is essential to establish a clear and coherent relationship between component identity and component type, as this underpins effective provenance tracking and prioritization. For instance, a component type, such as a software library, should be associated with a distinct component identity (e.g., a purl), enabling consistent identification and location of software packages across various programming languages, package managers, packaging conventions, tools, APIs, and databases.
Recommendation: Emphasize the importance of maintaining a clear and coherent relationship between component identity and component type, as this is fundamental for accurate provenance and effective prioritization.

Summary of Recommendations

FSSCC offers the following recommendations to enhance the 2025 SBOM Minimum Elements guidance to be both actionable and sustainable. These recommendations are intended to promote interoperability, reduce unnecessary complexity, and focus on elements that deliver meaningful risk reduction.

- Maintain alignment with SPDX and CycloneDX to preserve interoperability and usability across sectors.
- Designate as optional dependency relationships and tool name fields until their value is demonstrated in practice.
- Clarify the component hash field, ensuring suppliers specify the algorithm and software version.
- Add component manufacturer, SBOM manufacturer, component type, known unknowns as fields noted in the guidance, aligning with existing schemas.

- Ensure a clear relationship between component identity and type to support accurate provenance and prioritization.

The FSSCC supports CISA's leadership in advancing SBOM practices. By refining the minimum elements to prioritize actionable fields and ensuring schema alignment, CISA will help ensure that SBOMs remain usable, interoperable, and impactful in strengthening national cyber resilience.

We welcome continued engagement with CISA on this important initiative and remain available to provide further input as the guidance is refined.

Sincerely,
Debbie Guild, FSSCC Chair
Executive Vice President and Head of Technology, The PNC Financial Services Group