Subject: Response to CISA SBOM Minimum Elements Draft
Date: October 2, 2025
Submitted by: Zerberus Technologies Ltd
Contacts:

- Ramkumar Sundarakalatharan (ram@zerberus.ai)
- Sriram Gopalakrishnan (sriram@zerberus.co.uk)

ZERBERUS

Introduction to Zerberus

Zerberus Technologies is a cybersecurity and compliance automation company focused on securing the modern software supply chain. We are building a platform that integrates **Trace-AI** (metadata-driven SBOM and supply-chain risk engine), **Compl-AI** (compliance automation and evidence management), and **Remed-AI** (patent-pending "One-Click Remediation"). We have been working on the Software supply chain Security for 4+ years and have actively contributed to multiple open-source projects in this area.

Our products are designed for SaaS providers, scale-ups, and enterprises that need to align with standards like ISO 27001, SOC 2, PCI DSS, and the EU AI Act while managing risks in complex CI/CD environments. We are currently engaged with early adopters across the UK, US, and India, including SaaS firms in fintech, sports technology, and AI.

We commend CISA for continuing to refine the Minimum SBOM Elements to reflect industry progress and emerging technologies. While we strongly support many of the proposed updates in the draft, we respectfully recommend the following additions and clarifications to ensure SBOMs remain **actionable, verifiable, and future-proof**.

Comments on the CISA SBOM Minimum Elements Draft

We appreciate CISA's continued effort to enhance software supply chain transparency through this updated guidance. The revisions particularly the addition of new data fields like **License** and **Component Hash** and the introduction of **Coverage** reflect critical advances in SBOM maturity.

However, clarification is urgently needed regarding the machine-readable implementation of certain crucial new requirements, specifically those that rely on generic extensibility features within existing standards (SPDX and CycloneDX).

Need for Standardization of Non-Native Fields

The updated requirements include fields and practices that are not universally supported by single, dedicated atomic properties in current SBOM schemas. Instead, implementation requires using generic extension mechanisms (e.g., CycloneDX's *properties*]) or descriptive comment fields (*comment* in SPDX). Relying solely on these generalized fields without prescribed nomenclature introduces a significant risk to automation and interoperability, which CISA rightly identifies as critical for driving security at scale.

We request that CISA clarify or publish supplemental implementation guidance defining specific, standardized key names for the following minimum elements, ensuring they are machine-readable regardless of the specific format used:

1. Coverage and Feasibility of Transitive Dependencies

- **Challenge**: The requirement for full, unlimited-depth transitive dependency coverage is often impractical in complex software ecosystems like PyPI, NPM, and Maven, where dependency trees can contain thousands of nodes. This presents a significant adoption barrier for software producers.
- **Recommendation**: Introduce a tiered coverage model. Mandate **Core Coverage** for direct and first-order transitive dependencies, while designating deeper levels as **Extended Coverage** that can be provided where tooling supports it. This approach ensures a practical baseline for all producers while allowing for more comprehensive data where feasible.

2. Standardizing Generation Context

- **Challenge**: While SBOMs must now specify the software lifecycle phase (e.g., pre-build, post-build) at the time of generation, neither SPDX nor CycloneDX offers a native, standardized field for this purpose. This will lead to inconsistent reporting and complicates automated parsing.
- **Recommendation**: CISA should define a mandatory, standardized key-value convention (e.g., a reserved property name and controlled vocabulary) for expressing the Generation Context within the extension mechanisms of existing SBOM formats, ensuring uniform collection and consumption.

3. Differentiating Redacted vs. Unknown Data

- **Challenge**: Standard practices for handling missing data, such as using `NOASSERTION` in SPDX or omitting fields, fail to distinguish between information that is **intentionally**

redacted for confidentiality and data that is genuinely **unknown** to the author. This ambiguity can cause SBOMs to be incorrectly flagged as incomplete.

- **Recommendation**: CISA should standardize a machine-readable method, such as a designated field or value (e.g., `dataIntent: WITHHELD`), to explicitly mark components or properties as intentionally omitted. This allows automated tools to accurately interpret SBOM completeness, which is critical for systems handling proprietary or classified components.

Conclusion

The 2025 draft significantly advances SBOM maturity, especially through improved transparency and lifecycle context. To ensure **broad adoption and operational utility**, we urge CISA to adopt **tiered coverage models, clarify Known Unknowns risk handling**.

Zerberus Technologies stands ready to contribute further insights, particularly from our ongoing research into **metadata-driven SBOM risk classification (opensourced ZSBOM framework)** and real-world SaaS compliance automation.