REQUEST FOR COMMENT ON 2025 MINIMUM ELEMENTS FOR A SOFTWARE BILL OF MATERIALS

October 3, 2025

I. INTRODUCTION

In response to the Cybersecurity and Infrastructure Security Agency's ("CISA") request for comments on 2025 Minimum Elements for a Software Bill of Materials ("SBOM Minimum Elements document") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

CrowdStrike appreciates CISA's engagement with stakeholders and the opportunity to provide comments on the SBOM Minimum Elements documents. We agree with CISA's effort to update and review the SBOM Minimum Elements document to ensure it reflects the most useful information. As development teams continuously accelerate their software creation velocity, security remains paramount. CrowdStrike agrees with CISA's general statement in the request for comment document that the SBOM tooling landscape has expanded beyond SBOM generation to include other capabilities.

We do not have feedback on every question, but we do want to offer several points that may be of value to CISA.

A. Should any elements be removed from the 2025 CISA SBOM Minimum Elements, meaning the element should not be required for all SBOMs? Which elements, and why?

The SBOM Minimum Element document includes several additions and updates that will create new obligations for SBOM suppliers. In general, as CISA finalizes the minimum element requirements, the practicability and actionability of new requirements for agencies should be prioritized. The industry is moving towards more dynamic depictions of software elements; however, dynamic depictions are not always feasible especially where there are legacy products. *Generation Context* is a new minimum element introduced and would require data from the relative software lifecycle before build, during build, and after build. Requiring data regarding the before build stage could present operational challenges in certain contexts. We recommend industry continue investment in making dynamic depictions of such data available as feasible.

B. Software-as-a-service and Artificial Intelligence

The SBOM Minimum Elements document states that the document can also apply to Software-as-a-service ("SaaS") and Artificial Intelligence ("AI") software. CrowdStrike recognizes that while SBOMs provide valuable component transparency for traditional software, SaaS environments require a broader security framework that encompasses real-time posture monitoring, permission management, and behavioral analysis across hundreds of integrated applications. SaaS platforms are constantly changing and evolving, meaning a SaaS SBOM could be outdated moments after it is created. SBOMs represent one data point in a comprehensive SaaS security strategy, but effective protection depends equally on continuous visibility into security configurations, user behaviors, and access boundaries that change dynamically in cloud environments.

This approach emphasizes that static dependency mapping through SBOMs must be complemented by actionable security controls across multiple domains including access control, data leakage protection, endpoint protection, and automated remediation capabilities. The emerging best practice for SaaS security combines traditional software transparency with cloud-native risk management which can account for the rapid change cycles of modern software delivery.

CrowdStrike agrees that organizations must have a high degree of fidelity in their products and services - including AI. The SBOM Minimum Elements document notes that AI software SBOM is an area of ongoing exploration and future work. CrowdStrike supports CISA exploring AI security broadly and engaging with stakeholders throughout the process.

C. Software Security Best Practices

Modern software, and in particular cloud-based SaaS solutions, is much more likely to use a dynamic rather than static list of components. Components can number in the thousands depending on the complexity of the offering. Additionally, risk can vary significantly across components. These factors complicate both the practical ability to maintain an up-to-date list of each software component and the efficacy of using such information, thereby creating a signal vs. noise problem. Accordingly, there are other steps organizations can take to achieve the objective of enhancing supply chain security.

- *Application Security Posture Management* (ASPM). Supply chain security and the visibility of third-party components are often a challenge organizations want to solve with SBOM requirements. To address those challenges, we alternatively recommend leveraging an Application Security Posture Management (ASPM). An ASPM tool can provide runtime observability of third-party software libraries, offering visibility into code behavior after deployment, not just a static analysis,—a critical capability for managing the complex supply chain dependencies that characterize modern software development.

- *Zero Trust Architecture* (ZTA). As other CISA guidance reflects, ZTA concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. This constrains threat actors' ability to achieve actions on objective and provides additional opportunities for defenders to detect threats, making ZTA concepts core to the software security lifecycle. To be fully effective, ZTA concepts must be applied to developer's workstation and tools, in addition to the software being developed.

- *Integration of Threat Intelligence*. There is a growing complexity and volume of cyber threats targeting software development environments. Whether through supply chain attacks or otherwise, adversaries periodically breach even very-well defended enterprises. However, skilled defenders can find them and thwart their goals. Leveraging real-time threat intelligence is a leading indicator of the strength of an enterprise cybersecurity program. CrowdStrike's approach to secure software development is informed by real-world threat intelligence to provide unparalleled visibility into how adversaries actually operate in modern development environments. Leveraging this intelligence enables development teams to prioritize security efforts based on actual exploit likelihood rather than

theoretical Common Vulnerability Scoring System (CVSS) scores alone.

- *Artificial Intelligence* (AI). Leveraging best-in-class cybersecurity technologies deploying AI is essential to meeting constantly-evolving threats. Defenders can leverage AI in several ways throughout the DevSecOps lifecycle such as generating security and compliance artifacts, providing contextual remediation guidance, and enabling continuous monitoring across the entire software development lifecycle—from code commit to production deployment. By embedding these capabilities directly into existing continuous integration/continuous delivery pipelines and development toolchains, organizations can improve security without sacrificing development velocity and ultimately creating more resilient software through enhanced collaboration between development, operations, and security teams.

III. CONCLUSION

CISA's review of the SBOM Minimum Elements represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. With an emphasis on adoption of practical security practices, this update can raise the standard of cybersecurity across some of the most critical sectors. As CISA moves forward, we recommend continued engagement with stakeholders.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***