NETIMPACT STRATEGIES

Cracking the Code: How Strong Software Bills of Material (SBOMs) Can Mitigate Cyber-Supply Chain Risks

NetImpact Strategies, Inc.

7600 Leesburg Pike, West Building, Suite 140, Falls Church, VA 22043
(703) 559-3280 | www.netimpactstrategies.com

Introduction

In today's digital age, supply chains have become increasingly complex and interconnected adding to the cybersecurity risks that Agencies must grapple with. These are augmented by the growing use of open-source software and the potential licensing risks that come with it. A recent Center for Security and Emerging Technology (CSET) analysis of public government procurement records provided by GovSpend found that at least 1,681 state and local entities purchased equipment and services prohibited at the federal level under Section 889 between 2015 and 2021.

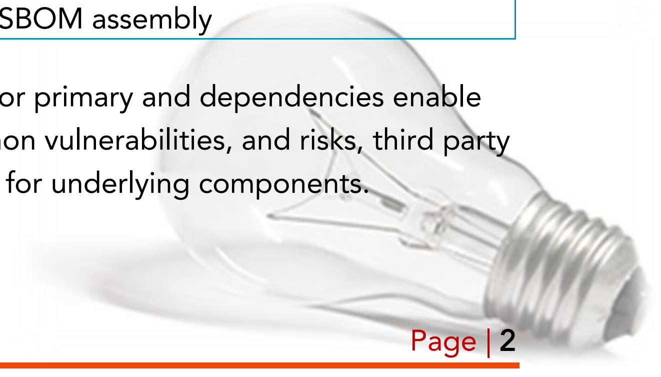
In the containing endeavor to battle these risks, Executive Order 14028, titled "Improving the Nation's Cybersecurity," was issued by President Biden on May 12, 2021. The order requires federal agencies to implement measures to improve the nation's cybersecurity and includes provisions related to Software Bill of Materials (SBOMs). What is an SBOM? How can it help make our nation more secure?

What Role Do Software Bills of Material (SBOMs) Play in Supply Chain Risk Management?

SBOM is a formal record containing the details and supply chain relationships of various components used in building software. A SBOM provides visibility into the software supply chain, enabling organizations to identify potential vulnerabilities and take appropriate measures to mitigate them. By understanding the components and dependencies of a software product, organizations can assess the risks associated with using that product and make informed decisions about its use. For instance, SBOMs provide preliminary details that Agencies can use to trace details on Suppliers such as geo-location, ownership, and performance. Using just this information, they can determine overall supplier diversity (supply chain resilience), potential geographical risks, and preliminary performance indicators and any red flags. Component and Component Version details for primary and dependencies enable an Agency to review for whitelisted components, common vulnerabilities, and risks, third party independent reviews, and any potential licensing issues for underlying components.

Minimum Elements of a SBOM

- **Supplier Name:** Name of entity that created, defined and identified the component
- **Component Name**: Title listed to component/software
- **Component Version**: Identifier of current component to specify variations
- **Other Unique Identifiers**: Software Identification that aid consumers find components in database
- **Dependency Relationship**: Show the relationship between the component and software
- **SBO Data Author**: Name of entity that created the SBOM
- **Timestamp**: Record of the date and time of SBOM assembly



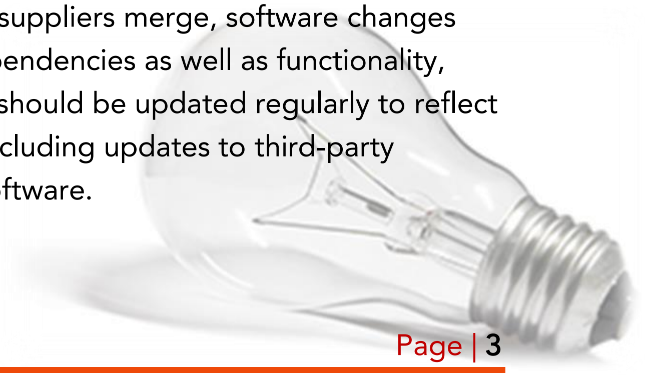
SBOMs also play an essential role in cyber security and incident response. SBOMs offer insight into potential vulnerabilities from Common Vulnerabilities Scoring Sites and allowing agencies to prioritize or mitigate vulnerabilities of software in their environment. In the event of a cyberattack or data breach, a SBOM can be used to identify the components of the software product that are affected. This information can be used to contain the attack and mitigate its impact.

EO 14028 mandates that software developers provide a SBOM for each software product they develop. This SBOM must be provided to the buyer and made available publicly. The order directed the National Institute of Standards and Technology (NIST) to develop standards, guidelines, and tools for the creation, management, and use of SBOMs.

How to Build a Robust SBOM?

An effective SBOM provides a comprehensive inventory of all the components and dependencies of a software product, including third-party components and open-source libraries. This information is essential for identifying potential vulnerabilities and ensuring the security of the software product. To build a strong SBOM, organizations should follow best practices for creating, managing, and using SBOMs. These include:

- **Create an accurate inventory:** Organizations should work with their software developers to create an accurate inventory of all the components and dependencies of their software products. This inventory should include information such as version numbers, licensing information for each component, other component derivative and dependent relationships, known vulnerabilities, lifecycle phase when the analysis was done (Source, Build or Post-Build), and cryptographic hash of component to validate it is a trusted version.
- **Investigate the Known-Unknowns:** Require the SBOM author to explicitly identify "known unknowns" i.e. identify dependency data draws a clear distinction between a component that has no further dependencies and a component for which the presence of dependencies is unknown and incomplete. This must be integrated into the automated data. To avoid erroneous assumptions, the default interpretation of the data should be that the data is incomplete; the author of the data should affirmatively state when the direct dependencies of a component have been fully enumerated, or when a component has no further dependencies.
- **Keep the SBOM up to date:** SBOMs are not static, suppliers merge, software changes ownership, new versions are released with new dependencies as well as functionality, and new vulnerabilities are introduced. The SBOM should be updated regularly to reflect any changes or updates to the software product, including updates to third-party components or open-source libraries used in the software.



- **Share the SBOM with stakeholders:** The SBOM should be shared with stakeholders, including buyers, partners, and regulatory agencies. This helps to increase transparency and accountability and enables stakeholders to make informed decisions about the security of the software product.
- **Verify the accuracy of the SBOM:** Organizations should verify the accuracy of the SBOM through regular testing and validation. This includes vulnerability scanning, penetration testing, and other security assessments.
- **Use a standardized format:** The SBOM should be created using a standardized format, such as SPDX (Software Package Data Exchange). This makes it easier for organizations to compare and share SBOMs and ensures consistency in the information provided.

In addition to these best practices, Agencies should also consider using automated tools to create and manage their SBOMs. These tools can help to streamline the process and ensure the accuracy and completeness of the SBOM. By following best practices for creating, managing, and using SBOMs, Agencies can increase their visibility into their software supply chains, identify potential vulnerabilities, and make informed decisions about the security of their software products.

NetImpact's DX360°® C-SCRM

NetImpact's DX360°® C-SCRM is a must-have tool for any Agency looking to navigate and mitigate risks in their complex supply chain. With DX360°® C-SCRM, Agencies regain the power of proactivity and the ability to reveal and neutralize threats – including ones traditionally obscured by the supply chain complexities. *Specifically, for SBOM, DX360°® C-SCRM empowers Agencies with the ability to digitally track systems components, technologies, supply sources, and automatically identifies risks with industry-published knowledge listings for continuous risk identification and remediation. Our SBOMs are generated in a machine-readable format built to NIST standards using Software Package Data Exchange (SPDX) 12, CycloneDX13, and Software Identification (SWID) tags.* DX360°® C-SCRM enables Agencies identify, evaluate, and assess risk factors, and make informed risk management decisions to achieve outcomes-focused compliance with NIST RMF and CSF, RMF for DoD IT, CNSS 1253, FedRAMP, ISO, and COBIT 5 guidelines. With a comprehensive library of potential risks and smart dashboards, C-SCRM provides real-time visibility into supply chain operations, including software security, and treatment plan recommendations to help you identify and treat potential risks that disrupt your supply chain ecosystem, which can threaten the entirety of your enterprise functions. DX360°® C-SCRM builds resiliency for your Agency with each step, from detection through treatment.

Request a Demo

Experience a live, customized demo with our experts to learn how DX360°® C-SCRM or our other DX360°® products will make your mission fulfillment goals easier and safer.

Our products are sold as Software-as-a-Service (SaaS), which means your subscription includes maintenance and upgrades, eliminating expensive capital investments in hardware and software. Additionally, our Microsoft DX360°® products effortlessly integrate into your existing tenant so it won't be bogged down by accreditation processes either. Experience immediate outcomes for mission value with rapid implementation in as little as two (2) weeks.

demo@netimpactstrategies.com

About NetImpact Strategies Inc.

NetImpact is a NextGen digital transformation leader disrupting how technology is applied to deliver mission value. Our team understands the challenges of managing and modernizing your agency's technology. That is why we have developed a portfolio of powerful, yet easy-to-use DX360°® apps that are designed to help you tackle your mission's most pressing needs. Building on our decades of experience in developing technology that integrates seamlessly into your ecosystem, we have harnessed the power of platforms from world-class partners like Microsoft to bring you a range of products for digital transformation in Government. These trailblazing applications are high-value, ready-to-use solutions tailored to federal missions and their evolving needs. Our DX360°® suite of high-performance digital solutions drives impact by delivering agile, outcome-focused results to securely transform client operations and accelerate mission outcomes at a fraction of the cost of traditional projects.