



WHITE PAPER

# SBOM Use Cases for Asset Owners

Insights from the North American Energy Software Assurance Database Initiative

Bryan Cowan  
Ty Short

July 2023

Fortress Information Security  
250 South Orange Ave. Ste. 500  
Orlando, FL 32801  
(407) 573-6800  
[sales@fortressinfosec.com](mailto:sales@fortressinfosec.com)

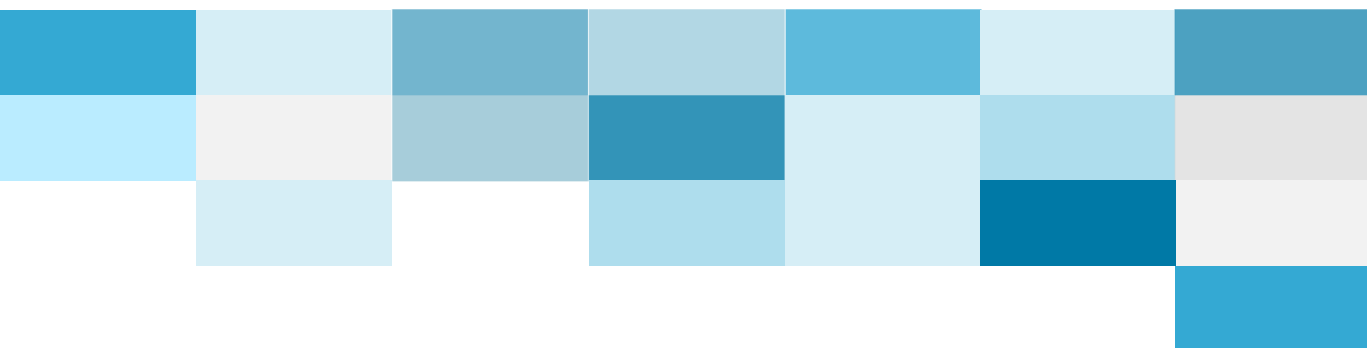


# BRIEF

Many cybersecurity guidelines, standards, regulations, and industry-specific guidelines prescribe the collection of Software Bills of Materials (SBOMs) by asset owners; however, there is presently minimal guidance on how to incorporate SBOMs into existing risk management processes for asset owners.

This document seeks to build upon existing guidance for SBOM use cases, such as the work documented by NTIA<sup>1</sup>, and apply the most up-to-date learnings from SBOM implementations in the North American Energy sector.

The document is intended to serve as a practical guide to understanding how SBOMs can be used by your organization.



---

<sup>1</sup> See 2019 publication from National Telecommunications and Information Administration (NTIA), *Roles and Benefits for SBOM Across the Supply Chain*, NTIA Multistakeholder Process on Software Component Transparency, Use Cases and State of Practice Working Group, available at [https://www.ntia.gov/sites/default/files/publications/ntia\\_sbom\\_use\\_cases\\_roles\\_benefits-nov2019\\_0.pdf](https://www.ntia.gov/sites/default/files/publications/ntia_sbom_use_cases_roles_benefits-nov2019_0.pdf)



## Table of Contents

<b>BRIEF .....</b>	<b>2</b>
<b>INTRODUCTION .....</b>	<b>5</b>
Context for SBOMs.....	5
Intended Audience.....	6
Sources .....	6
Building the Case for SBOM Adoption .....	6
<b>EXECUTIVE SUMMARY.....</b>	<b>8</b>
<b>USE CASE PRIMER .....</b>	<b>9</b>
Common Stakeholders .....	10
Top Use Cases by Asset Owners Today.....	11
Risk Areas Addressed by SBOMs .....	12
Common Tool Integrations .....	14
<b>IT/OT SECURITY USE CASES.....</b>	<b>15</b>
Vulnerability Incident Response .....	16
Third-Party Risk Management.....	18
Architecture Review .....	19
Threat Hunting .....	20
Vulnerability Management.....	22
<b>PROCUREMENT USE CASES .....</b>	<b>24</b>

Pre-Purchase Security Review .....	25
Contract Conditions.....	26
<b>COMPLIANCE USE CASES .....</b>	<b>28</b>
Licensing Compliance .....	29
Vulnerability Mandates.....	31
Attestation and SBOM Collection.....	33
<b>OPERATIONAL USE CASES.....</b>	<b>34</b>
Investing / Mergers & Acquisitions .....	35
Mission and Operational Readiness .....	37
Efficient Internal Code Development .....	38
<b>THE ROAD AHEAD .....</b>	<b>39</b>
Many Stakeholders, Little Awareness .....	40
Tool Maturity.....	40
<b>THE ROAD AHEAD .....</b>	<b>41</b>
<b>APPENDIX 1: CONTEXT FOR SBOM.....</b>	<b>43</b>
Introduction .....	44
<b>APPENDIX 2: SUPPLY CHAIN ATTACK EXAMPLES .....</b>	<b>49</b>
<b>APPENDIX 3: USE CASE QUICK REFERENCE .....</b>	<b>52</b>
<b>APPENDIX 4: REGULATIONS AND INDUSTRY GUIDELINES .....</b>	<b>55</b>
SBOM Regulatory Summary.....	68
<b>APPENDIX 5: SUMMARY OF INCENTIVES FOR ADVANCED CYBERSECURITY .....</b>	<b>69</b>
<b>APPENDIX 6: BUILDING A BUSINESS CASE.....</b>	<b>72</b>
<b>APPENDIX 7: SBOM RESOURCES .....</b>	<b>79</b>



# INTRODUCTION

## Context for SBOMs

Software supply chains are actively being exploited by sophisticated threat actors, and software end users bear the greatest burden of securing the software. See Appendix 1 for examples.

The first pillar of the Biden-Harris 2023 Cybersecurity Strategy<sup>2</sup>, announced on March 2, 2023, begins with shifting the burden of cybersecurity to those most capable of dealing with it – i.e., the software’s producer – followed by realigning incentives for long-term investments in security.

This follows the issuance of Executive Order 14028<sup>3</sup> Improving the Nation’s Cybersecurity (May 12, 2021) and the related OMB-22-18<sup>4</sup> (Sept. 14, 2022) with updates by the OMB-23-16<sup>5</sup> (Jun. 9, 2023) memorandum.

The FDA has also issued draft guidance for premarket submissions of medical devices<sup>6</sup>. The Edison Electric Institute’s Model Procurement Language, NERC Security Guidelines for Vendor Risk Management Lifecycle, and NERC Security Guidelines for Supply Chain Provenance all call for the collection of SBOMs.

Why are regulators calling for SBOMs? An SBOM, essentially an ingredients list of the components used in the software, represents one of the most substantial pieces of transparency – showing that secure software development practices are followed.

---

<sup>2</sup> White House. “Biden-Harris Administration Announces National Cybersecurity Strategy”. <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>

<sup>3</sup> GSA. “Executive Order 14028: Improving the Nation’s Cybersecurity”. <https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity>

<sup>4</sup> Office of Management and Budget. M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices. <https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf>

<sup>5</sup> Office of Management and Budget. M-23-16, Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices. <https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf>

<sup>6</sup> FDA. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff. <https://www.fda.gov/media/119933/download>

## Intended Audience

This document is designed to provide practical guidance to cybersecurity-minded business leaders who are considering the implementation of Software Bill of Materials (SBOMs) or those in working groups that are concerned with the topics of SBOM use cases, SBOM adoption, and supply chain cybersecurity.

Additionally, the document aims to provide insights into financially sustainable deployments of SBOM solutions while ensuring widespread organizational adoption and predictability throughout the process.

## Sources

The contents of this document have been informed by interviews of leaders in the North American Energy Software Assurance Database (NAESAD) initiative, who are contemplating or have already implemented SBOMs in their respective organizations. NAESAD was founded as a collaborative arrangement between North American power utilities with the purpose of working on standard methods for both buyers and suppliers in identifying, analyzing, and resolving potential software-related risks within the supply chain of software used by the members. The NAESAD initiative is especially focused on operational technology (OT), supervisory control and data acquisition (SCADA), cloud, and critical IT software, prioritized by the overlap between its asset owner members.

## Building the Case for SBOM Adoption

The widespread adoption of SBOMs is seen as inevitable by many cybersecurity professionals but there is concern about industry stakeholders making the necessary investments for feasible and sustainable SBOM adoption.

### Growing Adoption by Boards

The National Association of Corporate Directors (NACD) offers training for board members. In their latest handbook, 2023 Director's Handbook on Cyber-Risk Oversight, NACD highlights the necessity of using SBOMs as a key artifact in achieving the "use and write secure software" objective of designing and deploying technology securely<sup>7</sup>.

### Favorable Financial Treatment

In the context of financial reporting, it is frequently advantageous to categorize expenditures as capital investments rather than incurred expenses. This strategic classification allows an organization to effectively eliminate such expenditures from the widely used financial metric known as Earnings Before Interest, Taxes, Depreciation, and Amortization (EBITDA). Under Generally Accepted Accounting Principles (GAAP), investments in Software Bill of Materials (SBOMs) may potentially qualify for this capital treatment.

---

<sup>7</sup> National Association of Corporate Directors. 2023 Director's Handbook on Cyber-Risk Oversight, p. 86. [https://isalliance.org/wp-content/uploads/2023/03/Cyber-Risk-Oversight-Handbook\\_WEB.pdf](https://isalliance.org/wp-content/uploads/2023/03/Cyber-Risk-Oversight-Handbook_WEB.pdf)

This is largely because the information procured through such investments retains a tangible value and will continue to exhibit a useful life that extends beyond a single fiscal year. Therefore, in alignment with GAAP standards, such expenditures can be capitalized and systematically depreciated over the course of their useful life instead of being fully expensed in the year in which they were incurred.

Furthermore, sector-specific incentives may also be available. See Appendix 5 for incentives in the energy sector.

### **Financial Incentives**

There are certain sector-specific financial incentives and funding available for cybersecurity investments. Business leaders should evaluate all potential sources of subsidy and funding for their specific sector. Incentives available for U.S. power utilities are discussed in an Appendix 5.

### **Business Case**

In addition to growing support from boards, capital treatment, and potential financial incentives, the business case for the use of SBOMs stands on its own – promising strong returns for managing risk with this new set of software transparency tools in our toolkit. See Appendix 6 for detailed business cases.

# EXECUTIVE SUMMARY

In an era marked by escalating cyber threats and a seismic shift towards digital dependence, the integrity, transparency, and security of software supply chains have never been more vital. The widespread adoption of Software Bill of Materials (SBOMs) has emerged as not only a critical response to these challenges but also a strategic alignment with the President's new cybersecurity agenda, key regulatory directives, and growing corporate governance focus.

The recent Biden-Harris 2023 Cybersecurity Strategy heralds a profound realignment in how we approach cybersecurity, placing the responsibility firmly on the shoulders of software producers and recognizing SBOMs as a cornerstone of modern digital risk management. This follows a series of directives, from Executive Order 14028 to OMB memorandums, all pointing towards the pivotal role of SBOMs in enhancing transparency and fortifying security across sectors. SBOMs provide:

- Visibility into the components used in software, firmware, and open-source applications.
- Transparency into applications similar to the way food labels provide an ingredients list.
- Accountability to a software supplier's code security practices, dependence on legacy software, vulnerabilities, and foreign influence.
- Defense against software supply chain attacks which were previously impractical to monitor.

The urgency to adopt SBOMs is not only driven by regulatory pressures but underscored by a favorable financial landscape. A compelling business case is emerging, with evidence of substantial savings offsetting 33% to 55% of relevant IT security spend (see Appendix 6: Building a Business Case). The business case unveils a staggering \$40 billion challenge in the software supply chain. Coupled with potential sector-specific incentives and strategic capital treatment under Generally Accepted Accounting Principles (GAAP), investments in SBOMs offer organizations a rare convergence of risk mitigation and financial reward.

From utilities to healthcare, the call for SBOMs is resonating across industries (see Appendix 4: Regulations and Industry Guidelines for EEI, NERC, NATF, FDA, and OMB publications), embodied by initiatives such as the North American Energy Software Assurance Database (NAESAD). There is a shared recognition that SBOMs are essential to identifying, analyzing, and resolving potential software-related risks within the supply chain, especially in vital domains like operational technology (OT), supervisory control and data acquisition (SCADA), cloud, and critical IT software.

Despite this growing consensus, challenges remain. The path to feasible and sustainable SBOM adoption demands collective action, strategic investments, and industry-wide collaboration. The National Association of Corporate Directors (NACD) in its 2023 Director's Handbook emphasizes the necessity of using SBOMs in designing and deploying technology securely, signifying an evolving governance focus on this critical issue.

In conclusion, the adoption of SBOMs is not a matter of choice but an imperative. As our digital ecosystem becomes increasingly intricate and susceptible to sophisticated threats, SBOMs offer a potent solution that aligns with national strategy, satisfies regulatory compliance, and presents an attractive financial opportunity. The time to act is now, for the security of our digital future depends on the decisions we make today.

# USE CASE PRIMER

Software can be a black box; we simply don't know what components are used in products which run critical business operations. A way to improve that visibility is with a Software Bill of Material (SBOM), which is a machine-readable list of the components in a piece of software and includes things like supplier name, component name, and version. They can include information on relationships between components, licenses, and where each component came from.

For more information on the fields in an SBOM see the National Telecommunications and Information Administration's *The Minimum Elements for a Software Bill of Materials (SBOM)*<sup>8</sup> or a companion whitepaper from Fortress, *Software Bill of Materials (SBOM) Consumer Use Cases*<sup>9</sup>.

To provide examples of how SBOMs can be put into practice, we cataloged the following SBOM use cases which have been either implemented already or are under consideration by top US power utilities. The thirteen (13) use cases presented in this document are organized into four areas:

1. IT/OT Security – Relevant to security operations teams.
2. Procurement – Consideration and onboarding of software.
3. Compliance – Responding to regulations and industry guidelines.
4. Operational – Evaluating business and operational resiliency.

Each use case provides insight into how an asset owner may operationalize the implementation process. Additionally, see the accompanying Appendix 5 discussing potential ways SBOM investments can be rationalized through financial means.

Sections discussed in each use case include:

- Getting Started – Action items to be completed or considered prior to implementing the use case.
- Common Tool Integration – Potential integrations that can accelerate value delivery. All cases assume that an SBOM risk management solution will be employed to collect and generate SBOMs, produce comprehensive risk insights, and provide workflow for issue resolution.
- Description – Explanation of the use case.
- Example – Provides a representation of the process in operation.
- Summary Graphic – Overview of the steps for each use case.

---

<sup>8</sup> NTIA. *The Minimum Elements for a Software Bill of Materials (SBOM)*.

[https://www.ntia.gov/files/ntia/publications/sbom\\_minimum\\_elements\\_report.pdf](https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf)

<sup>9</sup> Fortress. *Software Bill of Materials (SBOM) Consumer Use Cases*. <https://www.fortressinfosec.com/en-us/sbom-consumer-use-cases-whitepaper>



# Common Stakeholders

Stakeholders in an organization can unlock value from investments in software supply chain transparency and security. Below are example groups that may or may not be applicable to your organization.

Stakeholder Department & Aliases	Responsibility
<b>Third Party Risk Management</b> <i>Vendor Risk Management</i> <i>Vendor Compliance</i>	Responsible for assessing, monitoring, and mitigating risks associated with outsourcing to third-party vendors or service providers to protect the company's assets and reputation.
<b>Security Assessments and Testing</b> <i>Penetration Testing</i>	Performs regular evaluations of the company's cyber defenses, using techniques such as penetration testing and vulnerability scans, to identify potential security weaknesses.
<b>Cybersecurity Consulting</b> <i>Cybersecurity Advisory</i> <i>Security Strategy and Governance</i>	Provides expert advice and strategic guidance on the implementation and improvement of the company's cybersecurity policies and practices.
<b>Vulnerability Management</b> <i>Security Operations Center</i>	Systematically identifies, classifies, prioritizes, and resolves security vulnerabilities to maintain the integrity, confidentiality, and availability of the company's digital assets.
<b>Cybersecurity Architecture and Design / Engineering</b> <i>Cybersecurity Infrastructure</i>	Designs and implements robust cybersecurity infrastructures, incorporating the latest security controls to protect the company's systems and data.
<b>Threat Intelligence and Response</b> <i>Security Operations Center</i>	Proactively monitors for potential cyber threats, coordinates incident response activities, and disseminates threat intelligence to appropriate teams within the company.
<b>Investment Strategy</b> <i>Portfolio Management</i> <i>M&amp;A / Strategy</i>	Works to balance risk and return in the company's investment portfolio, employing strategies to maximize value, improve performance, and ensure alignment with the company's financial goals.
<b>Procurement</b> <i>Supply Chain Management</i> <i>Purchasing</i>	Oversees the acquisition of goods and services required for the company's operations, ensuring quality, cost-effectiveness, and adherence to the company's procurement policies.
<b>Software Development</b> <i>Software Engineering</i> <i>Application Development</i>	Designs, builds, tests, and maintains software applications that support the company's operations, customer service, and strategic initiatives.
<b>Application Portfolio Mgmt.</b> <i>Enterprise Applications Mgmt.</i> <i>IT Management</i> <i>Business Solutions Services</i>	Develops and manages a suite of business applications and software solutions designed to streamline processes, improve productivity, and provide data-driven insights to support decision-making within the company.



# Top Use Cases by Asset Owners Today

Fortress interviewed SBOM solution buyers across the energy and defense sectors. **The top-three most urgent use cases identified were:**

1. Vulnerability Incident Response (Security)
2. Third-Party Risk Management (Security)
3. Attestation and SBOM Collection (Compliance)

## Respondent Organizations

		1	2	3	4	5	6	7	8
IT/OT Security	★ Vulnerability Incident Response	High	High	High	High	High	High	Low	Low
	★ Third-Party Risk Management	High	Med	Med	Med	Med	Low	Low	Low
	Vulnerability Management	Low	Low	Low	Low	Low	Med	Low	Low
	Architecture Engineering	Med	Low	Low	Low	Low	Low	Low	High
	Threat Hunting	Low	Low	Low	Low	Low	High	Low	High
Procurement	Contract Conditions	Med	Low	Low	Low	Med	Low	Low	Low
	Pre-Purchase Security Review	Med	Low	Low	Low	Med	Low	Low	Low
Compliance	Vulnerability Mandates	Med	Low	Low	Low	Low	Med	Low	Low
	License Compliance	Low	Low	High	Low	Low	High	High	Low
	★ Attestation & SBOM Collection	High	Med	High	Med	High	High	Low	Low
Operational	Mission and Ops Readiness	Med	Low	Low	Low	Low	Low	Low	High
	Investing (M&A)	Med	Med	Low	Low	Low	Low	Low	Low
	Efficient Internal Code Development	Med	High	Low	Low	Low	High	Low	Low

## Risk Areas Addressed by SBOMs

SBOM tooling for assessing software risks should include the areas listed below for comprehensive risk identification. This tooling is used throughout the use cases discussed in this document.

### **Vulnerability – Severity, Exploitability, and Reachability**

In order to determine the severity of potential vulnerabilities, each component of the software – including its international equivalents and private sources – should be evaluated against published vulnerability databases such as the National Vulnerability Database (NVD).

Vulnerabilities should then be evaluated for exploitability using sources such as CISA's Known Exploited Vulnerabilities (KEV) catalog and the Forum of Incident Response and Security Team's (FIRST) Exploit Prediction Scoring System (EPSS).

To reduce false positives caused by vulnerabilities that might be present but not reachable (due to inoperative functions or other reasons), reachability should be evaluated. Reachability is presently a challenge when evaluating third-party software, as automated methods are still in the early stages of development. Vulnerability Exploitability eXchange (VEX) is one solution where a supplier can be used to indicate the status of a software or software component with respect to vulnerability (e.g., affected, not-affected, etc.) – since they can more easily determine reachability through analysis of their own source code.

### **Dependency – Obsolescence, Security, Reliability/Maintainability**

Software should be built upon well-maintained code. The Linux Foundation estimates that 70%-90% of any given piece of modern software solutions utilize free and open-source software (FOSS) as a dependency<sup>10</sup>. FOSS should be evaluated for being up to date, how well it is being supported, if there are any known compromises or malware, the reputation of those contributing to it, the appropriateness of its code review practices, and that its upstream dependencies are also up to date.

In some cases, dependent FOSS will be abandoned, causing significant concerns for downstream consumers. This issue has become so prevalent that there are now companies that will broker transactions between FOSS communities and commercial software providers to ensure that FOSS is actively maintained.

### **Malware – Compromises, Malicious Maintainers**

All FOSS used should be evaluated for code contributions from a list of known or suspected malicious contributors, source code compromises, malicious packages, and build system compromises. Open-Source Security Foundation's (OpenSSF) Scorecard, for example, is one tool that

---

<sup>10</sup> Linux Foundation. "The Security of the Open-Source Software Digital Supply Chain: Lessons Learned and Tools for Remediation." <https://www.linuxfoundation.org/blog/blog/the-security-of-the-open-source-software-digital-supply-chain-lessons-learned-and-tools-for-remediation>

the industry uses to evaluate risks in FOSS. Additional malware scans should be performed on the compiled software as well.

### **Integrity – Component Hash Validation**

Most methods for identifying vulnerabilities rely on proper fingerprinting of software. If an SBOM includes a dependency but the hash value of the dependency does not match the source's hash value, this means the code may have been altered, and there could be hidden risks such as malicious code or vulnerabilities.

### **Licensing – Compliance, Obligation Tracking**

There are certain standard software licenses that bring obligations with them. Examples include the GNU General Public License (GPL) that requires any software that includes the license to also be made available under the same license (known as copyleft). Mozilla Public License (MPL) allows for code modifications, as long as any code licensed under the MPL is kept in separate files and these files are distributed with the software. There are several other licenses with variations of these requirements. SBOM analysis tooling should indicate these obligations.

### **Foreign Presence – Influence from Adversaries**

Through various U.S. Government publications<sup>11</sup>, China, Cuba, Iran, North Korea, Russia, and Venezuela have been designated as foreign adversaries that “have engaged in a long-term pattern or serious instances of conduct significantly adverse to the security of the United States....” All code used should be evaluated for any potential influence from these adversaries (e.g., reviewing code contributors, reviewing affiliations of commercial entities contributing to software dependencies).

### **Attestation for Secure Software Development – Governance**

NIST SP 800-218, Secure Software Development Framework, was released on February 3, 2022, as a framework for developing secure software throughout five phases of development: planning, architecture & design, implementation, testing, and deployment & operations. By using this framework, software producers (and their customers) can expect their software to have a lower risk of vulnerabilities, increased security, and long-term security cost savings from applying a secure-by-design approach.

CISA is preparing a Secure Software Self-Attestation Common Form to be used by suppliers to attest that key practices of NIST SP 800-218 are being followed. In general, suppliers selling software to U.S. government agencies will be required to attest to these practices under Executive Order (EO) 14028 and subsequent Office of Management & Budget (OMB) Memo No. M-22-18 and OMB Memo No. M-23-16.

---

<sup>11</sup> U.S. Department of Commerce. *Securing the Information and Communications Technology and Services Supply Chain*. <https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain>

## Common Tool Integrations

These integration tools provide ways to maximize the value of SBOM investments:

Tool	How to Leverage in SBOM Workflows
<b>Configuration Management Databases (CMDBs)</b>	Provides a master listing of applications that can be used to ensure that the SBOM collection is complete and current. When combined with SBOM component-level inventory, a single component can be traced to all affected assets.
<b>Software Asset Management (SAM) Systems</b>	Like a CMDB, the SAM will provide an inventory of all software utilized throughout the organization, which can be used to ensure that the SBOM repository is comprehensive.
<b>Vulnerability Scanners &amp; Sensors</b>	Many environments may not have sophisticated CMDB or SAM systems; thus, existing vulnerability management tools can be leveraged to identify software inventory to compare against the SBOM repository for completeness.
<b>Endpoint Detection &amp; Response (EDR)</b>	EDR systems are another way to identify a software inventory. In some cases, EDR tooling will be able to generate “deployed” SBOMs, which can be further compared to supplier-provided source or build SBOMs as well as the analyzed SBOMs.
<b>Security Information and Event Management (SIEM)</b>	SIEMs are a popular aggregation tool that helps organizations detect, analyze, and respond to security threats. Thus, embedding SBOM data can provide Managed Detection and Response (MDR) or Security Operations Center (SOC) teams with additional and relevant contexts.
<b>Procurement Systems</b>	As new Requests for Proposals/Information (RFPs/RFIs) are sent, procurement teams can request that SBOMs be provided as part of the submittal while also generating and analyzing SBOMs on the actual software files.
<b>Vendor Risk Management System</b>	Third-party risk management systems send out questionnaires and request artifacts from suppliers about various topics such as cybersecurity along with financial, operational, environmental, social, governance, regulatory, and performance issues. Attestations about secure software development lifecycles and the SBOM artifact are natural extensions.
<b>Governance, Regulatory, and Compliance (GRC) Systems</b>	Housing all SBOMs in a GRC will ensure that entities required (OMB-22-18/23-16 or FDA) or heavily encouraged (such as NERC Security Guidelines <sup>12</sup> ) to collect SBOMs can evidence that the required procedures took place with full audit logging.
<b>Developer Tooling (IDEs, SCA, and CI/CD)</b>	At each point in the development lifecycle (requirement analysis, plan, design, build, test, release, maintain), SBOM insights will aid development to deliver more reliable and secure code while maintaining higher velocity in the long run. When integrated with SBOM analysis tooling, Integrated Development Environments (IDEs) can provide real-time feedback during the coding phase. Also, Software Composition Analysis (SCA) tools can provide in-depth issue tracking; and Continuous Integration / Continuous Development (CI/CD) tooling can provide pre- versus post-build SBOM analysis.
<b>Supply Chain Risk Management Systems</b>	For precise and comprehensive cyber risk management in supply chains, systems should incorporate detailed SBOM risk analyses for enhanced component-level insights.

Other less common integrations could include Intrusion Detection & Prevention Systems (IDPS), patch management/deployment tooling, and contract management systems.

---

<sup>12</sup> See Appendix 4 for details on NERC Guidelines for Supply Chain Provenance and Vendor Risk Management Lifecycle – both referencing the collection of bills of materials.

# IT/OT SECURITY USE CASES



# Vulnerability Incident Response

## Getting Started

- Identify all stakeholders of asset inventory
- Identify vendor contacts for purchased software
- Plan for how application inventory will be collected to ensure SBOM coverage

## Summary

Traditional methods to vulnerability incident response can take weeks with high pressure and many unanswered questions. Having an up-to-date inventory of SBOMs from suppliers – and generated from the software itself – moves response duration from weeks to hours<sup>13</sup>.

**Answers:** *Am I impacted by Log4j?*

## Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: Yes
- Malware: Yes
- Licensing: n/a
- Foreign Presence: Yes
- Attestation: n/a

---

**Common Tool Integrations:** CMDB • SIEM • EDR

## Description

Traditional methods to identifying applicability of component level vulnerabilities include (i) scanning assets as plugins become available, (ii) log analysis, (iii) network monitoring for unusual spikes in traffic, (iv) remote log in and inspection, (v) onsite inspections (documentation, config files, interviews), (vi) penetration testing for exploitability, and (vii) poring through intelligence feeds.

SBOMs, especially those enriched by SBOM tooling, provide an inventory of the software components. This inventory can be searched to identify vulnerable components. This approach is demonstrably more efficient and effective than legacy methods.

## Example

Significant disruption was caused when critical severity vulnerabilities were discovered in Apache Log4j in December 2021. Log4j is a popular Java logging utility embedded in many commercial and

---

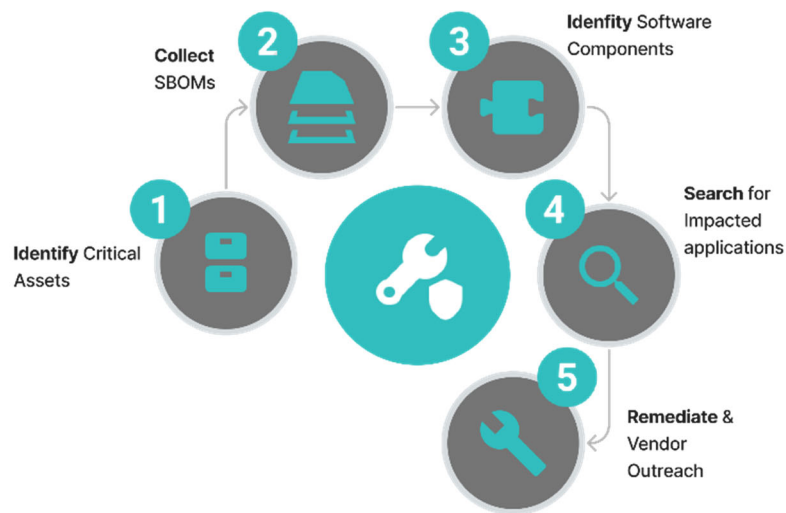
<sup>13</sup> At the SBOM-a-Rama event on June 14, 2023, in Los Angeles, a speaker representing a large manufacturer announced that with their up-to-date component-level software inventory, response time was under 4 hours, and that internal software development teams were able to deploy fixes within 2 weeks. This was a software producer scenario. Software consumers can benefit similarly with an up-to-date inventory.



open-source software. Organizations expended valuable time and resources to discover whether they were affected.

Using SBOMs as an up-to-date inventory, an incident response team can proactively identify which assets are affected by new vulnerabilities, prioritize mitigation for critical assets, and reach out to vendors whose products are impacted.

### Process Diagram



# Third-Party Risk Management

## Getting Started

- Identify all providers of software
- Identify internal contacts
- Identify vendor contacts for SBOM collection
- Inform business buyers of changes to the security requirements for software transparency
- Establish criticality ranking for software vendors

**Common Tool Integrations:** Vendor Risk Management System • Procurement System • GRC

## Description

By requesting SBOMs and secure software development attestations from third-party vendors, organizations can gain insights into the components and versions of software used in the vendor's products or services. This information helps assess the security posture of the software supply chain and identify potential vulnerabilities or risks associated with the vendor's offerings. For example, do any of the products use components that are outdated? Do any of components have one or more critical unpatched vulnerabilities? Do any of the components have unacceptable foreign influence?

## Summary

SBOMs can assist in assessing the security posture of third-party software suppliers and vendors. By requesting SBOMs from suppliers and reviewing the components and vulnerabilities present, organizations can make informed decisions about the security and trustworthiness of the software they integrate into their systems.

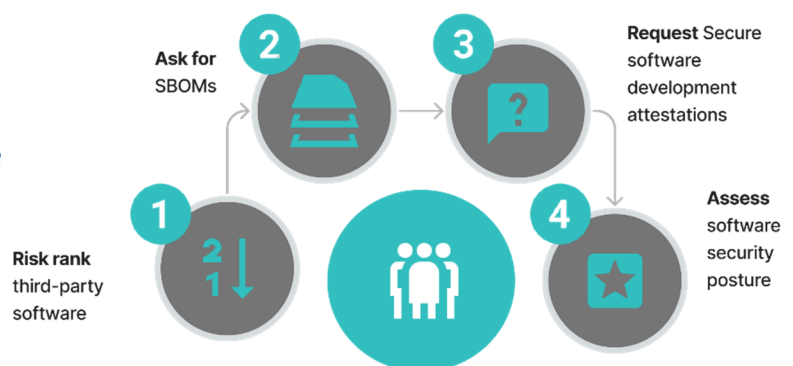
**Answers:** *Are my suppliers practicing secure software development?*

## Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: Yes
- Malware: Yes
- Licensing: n/a
- Foreign Presence: Yes
- Attestation: Yes

## Example

A utility company can use an SBOM to identify all third-party software components used in its industrial control systems. This information can then be used to assess the cybersecurity risks associated with these components and implement appropriate security controls.



# Architecture Review

## Getting Started

- Require SBOMs as part of the architecture review process
- Prepare standardized questionnaires based on findings identified in SBOM
- Establish scoring thresholds for software comparability

## Summary:

SBOMs provide a comprehensive inventory of the software components and dependencies used in an application. By analyzing the SBOM, organizations can review product policy concerns before installation, and ensure that the architecture is secure and reliable.

**Answers:** *What risks should I be aware of before I install or use this software?*

## Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: Yes
- Malware: Yes
- Licensing: Yes
- Foreign Presence: Yes
- Attestation: Yes

**Common Tool Integrations:** Cyber Risk Management System • Procurement System • GRC

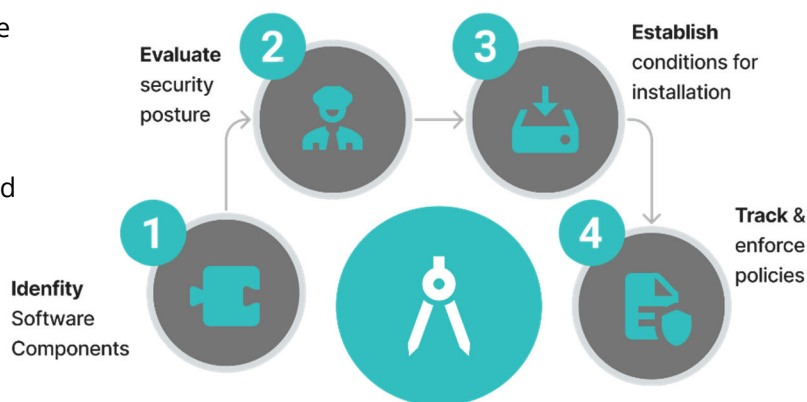
## Description

SBOMs can be used to verify the software components before deployment in an organization's IT architecture. This process can help verify that the software used by the organization is consistent with their security policies and standards. In an architecture review, an SBOM can be used to evaluate the security posture of an IT architecture by identifying known vulnerabilities.

A review of the dependencies between these components could identify the risk of a single component failure or vulnerability impacting the overall architecture. Additionally, SBOMs can be used to track and evaluate license compliance governing the use of open-source components.

## Example

A financial services company can use an SBOM to identify all the third-party software components used in its trading platform. This information can then be used to enforce the organization's IT policies against using insecure versions of common components, such as Apache Struts v2.3.5.



# Threat Hunting

## Getting Started

- Create process to compare deployed SBOMs with expected SBOMs
- Establish a plan of action for each type of unexpected variance

## Summary:

Threat hunting teams can use SBOMs to enable visibility into the supply chain during threat hunting operations. SBOMs aid in the identification of vulnerable components in software, allowing threat hunters to scope their work. Threat hunting teams tracking threat actors and their techniques can use SBOMs to scope potential impacted software and systems, given that these actors often exploit identical vulnerabilities across systems.

**Answers:** *Has my installed software been used to compromise my environment?*

## Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: Yes
- Malware: Yes
- Licensing: n/a
- Foreign Presence: n/a
- Attestation: n/a

**Common Tool Integration:** EDR/XDR • Endpoint Agents • SIEM/SOAR

## Description

SBOMs can be used by threat hunting teams to pinpoint software components that are known to be targeted by attackers. Threat hunting teams can combine SBOMs with data points such as the CISA KEV list, threat intelligence, asset inventory, EDR (where available in the OT environment), application logs, and network security monitoring logs, to build a holistic picture of their attack surface. This provides actionable insights into potential weak spots in the system that could be exploited by adversaries.

If a particular piece of software has been identified as being part of an attack campaign, threat hunters can use the SBOM to identify other software and systems that might also be at risk. Threat actors often exploit the same vulnerabilities in multiple systems and applications. By knowing the full scope of the organization's exposure, threat hunters can scope and prioritize their work.

## Example

Threat hunting teams learn of a new supply chain attack targeting a certain version of a component found in a piece of software. Teams query their SBOM database to identify potentially affected systems and begin proactive hunting operations. Teams also query for other software using affected versions and begin hunting based off those results.

# Vulnerability Management

## Getting Started

- Incorporate component vulnerabilities into vulnerability management
- Establish methods to reduce false positives
- Incorporate VEX collection from vendors

## Summary:

With SBOMs in hand, vulnerability management tools and platforms can compare the listed components against known vulnerability databases. This allows organizations to prioritize vulnerabilities based on their respective severity, reachability, exploitability, and business impact of the affected devices.

## Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: n/a
- Malware: Yes
- Licensing: n/a
- Foreign Presence: n/a
- Attestation: n/a

## Common Tool Integration: Vulnerability Scanners & Sensors • SIEM • CMDB

### Description

SBOMs can be used to search for known vulnerabilities and to identify software components in a system as well as the corresponding version numbers and other metadata.

Remediation efforts can be prioritized considering the severity of the vulnerability, the number of systems affected, and the likelihood of exploitation using VEX documents. Progress of remediation can be tracked by monitoring vulnerabilities – which have been patched and which have not.

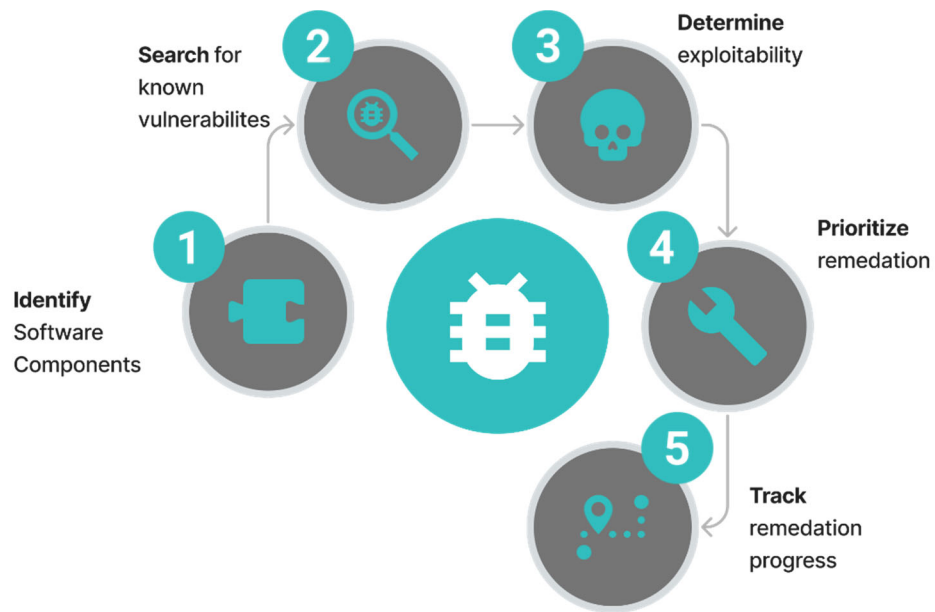
### Example

A security analyst performs a vulnerability scan, which also identifies installed software. The SBOMs for that software are collected from suppliers along with a VEX document through the third-party risk management team. SBOM analysis tooling identifies many component-level vulnerabilities that could include false positives.

Using a reachability analysis, along with the VEX document from the supplier, eliminates many of the potential false positives. The remaining vulnerabilities identified by the SBOM analysis tooling, previously unknown to the scanners, are then combined with additional context to prioritize remediation efforts.

A workflow is also initiated with the vendor to encourage the release of a security patch.







# PROCUREMENT USE CASES



## Pre-Purchase Security Review

### Getting Started

- Require software attestations, SBOMs, and VEX as part of RFX processes
- Connect with architecture review processes

### Summary:

SBOMs can be used during the software vendor selection process to evaluate the risks associated with software components. Reviewing the SBOM can provide insights into potential risks posed by software components, such as the use of outdated software versions, software with known vulnerabilities, or components with a history of security incidents.

**Answers:** *Are there avoidable security issues in the software I am potentially acquiring?*

### Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: Yes
- Malware: Yes
- Licensing: Yes
- Foreign Presence: Yes
- Attestation: Yes

### Common Tool Integration: Procurement Systems • Vendor Risk Management Systems

#### Description

Requesting an SBOM from a vendor should be part of the procurement evaluation process. A vendor's ability and willingness to provide this information can indicate the level of transparency and maturity of their software development life cycle (SDLC) and provides the illumination necessary to negotiate contractual software fixes.

SBOMs can be used to evaluate security posture and understand if any of the product's components are outdated or if they contain critical unpatched vulnerabilities.

#### Example

A healthcare organization creates an RFP for a new electronic health record (EHR) system. Five vendors are participating in the RFP, but only three were willing to provide an SBOM. Of the three, two demonstrate substantial security concerns. Through the RFP process, one agrees that they will be willing to fix the issues. Thus, the healthcare organization is armed with new information to make an informed decision.



## Contract Conditions

### Getting Started

- Create standard contract language for secure software development
- Create playbook for supplemental language for findings

### Summary:

SBOMs provide valuable information that can inform the decision-making process during procurement. Organizations can use SBOMs to compare different software options, assess their security and risks, and make informed choices.

Additionally, SBOM information can be used for negotiation purposes, ensuring that security requirements, vulnerability management practices, and compliance obligations are adequately addressed in vendor contracts.

**Answers:** *Are my suppliers fixing critical issues?*

---

### Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: Yes
- Malware: Yes
- Licensing: Yes
- Foreign Presence: Yes
- Attestation: Yes

**Common Tool Integration:** Procurement Systems • Vendor Risk Management System • Contract Management System

---

### Description

Different solutions can be compared to understand which product has the fewest security issues and to investigate if there are significant differences between vendors and how they have responded to discovered issues previously.

After deciding upon a product, SBOM analysis data can be used to manage risk during the contracting process. For example, the purchase agreement can include a term that requires the supplier to remediate component

vulnerabilities within a mutually agreed upon time frame. Or, if this is not feasible, buyers may instead ask to be appropriately compensated for the transfer of risk. Compensation may be in various forms, such as cost reduction, additional services, or extended support.

## Example

The software purchase being contemplated has a transitive dependency on a library that will become end-of-life for security updates in two months. The supplier has already been made aware of this issue during the procurement process and agreed to remediate. The contract is appended to include a guarantee with financial penalties if the library is not updated to a supported library within six months of contract execution.





# COMPLIANCE USE CASES





# Licensing Compliance

## Getting Started

- Create playbook for licensing issues
- Ensure business leaders are aware of licensing requirements
- Get plugged into procurement and application inventory processes

## Summary:

Ensure that internally developed and procured software is free of restrictions and obligations. By providing visibility into the software supply chain and the licenses that govern it, SBOMs can help organizations identify and address any potential compliance issues before they cause problems.

**Answers:** *Do we have hidden obligations in our software?*

## Relevant Risk Areas

- |                      |                         |
|----------------------|-------------------------|
| • Vulnerability: n/a | • Licensing: Yes        |
| • Dependency: n/a    | • Foreign Presence: n/a |
| • Integrity: n/a     | • Attestation: n/a      |
| • Malware: n/a       |                         |

**Common Tool Integration:** Supply Chain Risk Management Systems • Developer Tooling • Vendor Risk Management System

## Description

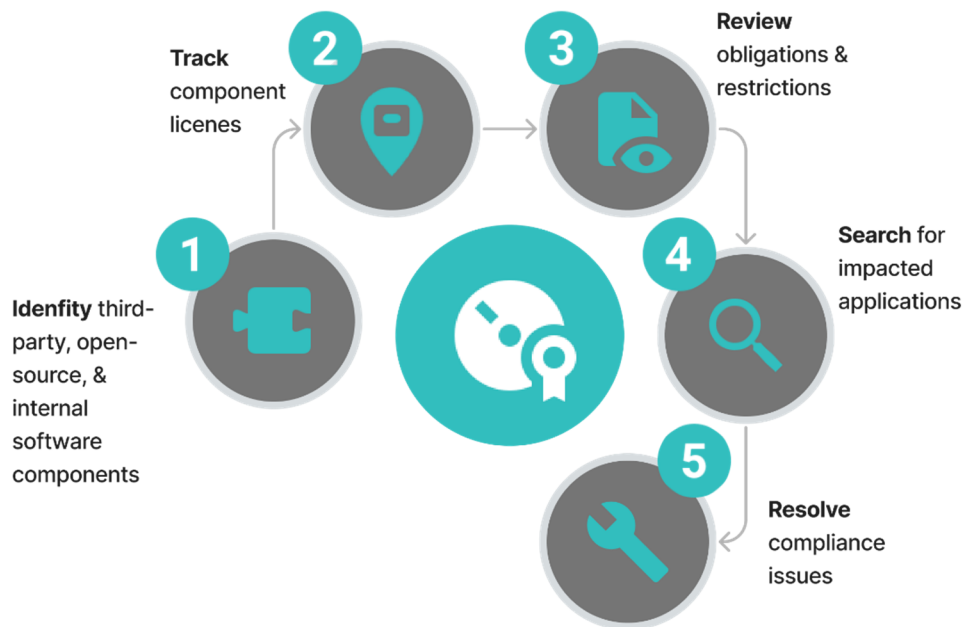
Asset owners may be software developers themselves and pull in code from partners and open-source components into their products. Many of these components come with license agreements that need to be tracked to ensure their use complies with their licensing terms.

This information can be utilized for internal audits, license compliance reviews, and reporting purposes. It helps organizations demonstrate due diligence in managing software licenses and meeting compliance requirements.

SBOMs provide information about the licenses associated with software components. Reviewing the SBOM allows organizations to identify the specific licenses that apply to each component – including open-source licenses, commercial licenses, or proprietary licenses – to understand any obligations or restrictions imposed by the licenses. These may include requirements for attribution, distribution of source code, limitations on usage, etc.

## Example

A manufacturer can use SBOMs to review and track the licenses of components in software from open-source libraries, third-party vendors, internally developed software, and partner companies. By proactively checking compliance with license terms, they can avoid costly, and time-consuming litigation.



# Vulnerability Mandates

## Getting Started

- Assess when and how regulations such as NERC CIP-010 or TSA Security Guidelines may incorporate component vulnerabilities
- Create data pipelines into existing systems for vulnerability management, but track separately to avoid overwhelming current processes

## Summary:

Both the Transportation Security Administration (TSA) and North American Electric Reliability Corporation (NERC) have requirements for vulnerability management. NERC has already published two documents recommending the adoption of SBOMs into procurement practices. See Appendix 4 for more information. While component-level vulnerabilities are not explicitly in scope today (some may argue there could be an implicit requirement), proactive organizations may adopt ahead of regulation.

**Answers:** *Am I ready for regulations to incorporate component vulnerabilities?*

## Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: Yes
- Malware: Yes
- Licensing: n/a
- Foreign Presence: n/a
- Attestation: n/a

**Common Tool Integrations:** GRC Systems • Vendor Risk Management System • Supply Chain Risk Management Systems

## Description

The TSA issues cybersecurity requirements for critical infrastructure organizations to implement measures like vulnerability assessments on a regular basis to identify all known vulnerabilities in systems and networks. NERC has regulations for vulnerability and patch management, as well as multiple security guidelines that recommend SBOM collection from suppliers<sup>14</sup>.

## Example

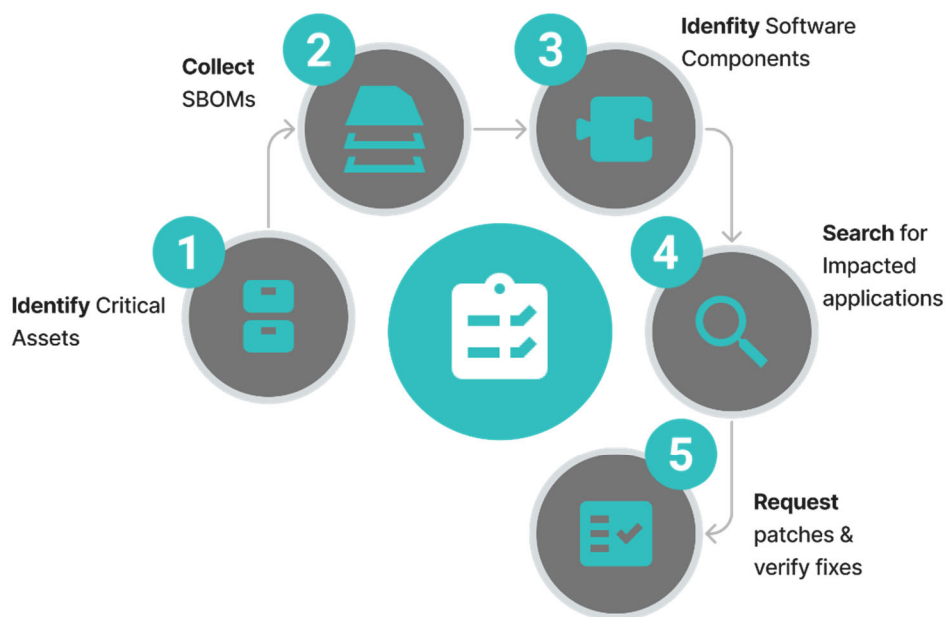
An investor-owned utility (IOU) requires vendors to provide SBOMs as part of a procurement process and on a going basis. The IOU also has a robust vendor risk management program.

The IOU uses the output from an SBOM analysis solution, which identifies the vulnerabilities in components, assesses for reachability, applies VEX documents, and evaluates exploitability & severity.

<sup>14</sup> See Appendix 4 for details on the NERC Security Guidelines – Vendor Risk Management Lifecycle and Supply Chain Provenance

As an up-to-date component inventory on critical assets, an SBOM can be used to identify known vulnerabilities on assets and all included components.

The remaining vulnerabilities are fed into a consolidated system of both software and component vulnerabilities. The component vulnerabilities are then prioritized only for the most critical assets to confirm exploitability and then apply appropriate mitigations. Workflows are also sent to the third-party risk management team, who will follow up with the vendor to encourage patches.



## Attestation and SBOM Collection

### Getting Started

- Understand timelines for compliance
- Create an inventory of all software used
- Special considerations for federal agencies (e.g., critical vs non-critical software)
- Identify supplier contacts
- Establish process for identifying major version changes

### Summary:

Customers and regulators are looking for transparency so they can better secure the software that powers their everyday operations. Scalable and secure sharing methods encourage sharing and collection of SBOMs and provide actionable information for specific environments.

**Answers:** *Am I compliant with software transparency mandates or best practices?*

### Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: Yes
- Malware: Yes
- Licensing: n/a
- Foreign Presence: Yes
- Attestation: Yes

**Common Tool Integration:** EDR • CMDBs • Procurement Systems, Vendor Management Systems • Vulnerability Scanners & Sensors

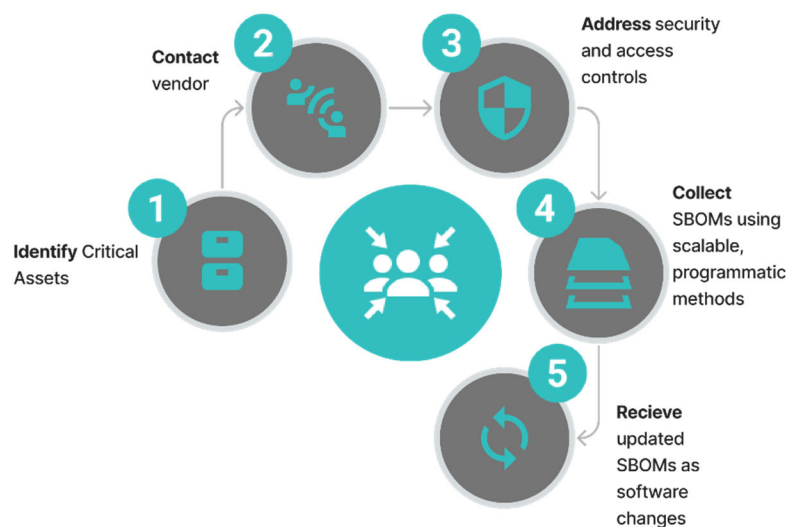
### Description

The Food and Drug Administration (FDA) will require SBOMs before approving new medical devices in October 2023. Additionally, North American Electric Reliability Corporation (NERC) has issued guidance on supply chain provenance, which recommends requiring vendors to provide SBOMs for current software and updated versions when the software changes.

Secure and permissioned sharing models reduce the concerns among vendors about data being provided to parties other than customers. Additionally sharing must be scalable and automated to support current versions of a product's SBOM, as software can be updated many times over its lifecycle.

### Example

An automaker contracts with a SBOM services provider to collect SBOMs on products from Tier 1 supplier. The service provider aggregates SBOMs from vendors via an authenticated API connection and receives permission from the Tier 1 supplier before furnishing the document to their mutual customer.





# OPERATIONAL USE CASES



## Investing / Mergers & Acquisitions

### Getting Started

- Due Diligence insights
- Improved Risk Management
- Decision-making support

### Summary:

SBOMs can be used as part of due diligence and decision-making practices in investment or mergers and acquisitions (M&A) use cases, to assess software-related risks and opportunities associated with target companies.

### Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: Yes
- Malware: Yes
- Licensing: Yes
- Foreign Presence: Yes
- Attestation: n/a

**Common Tool Integration:** Developer tooling • Supply Chain Risk Management Systems • CMDBs • SAM • Vulnerability Scanners & Sensors

### Description

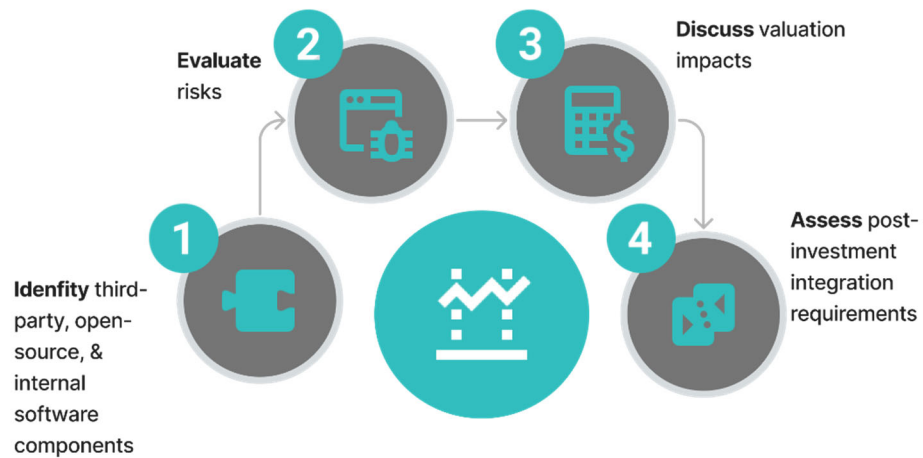
SBOMs provide valuable insights into the software components and dependencies used by a company that is a target of an M&A deal. By reviewing the SBOM, investors or acquirers can gain a clearer understanding of the software landscape, including the technologies, licenses used, and their related potential risks. This SBOM-supported risk information can be used to evaluate the quality, reliability, and security of the software assets of the target company. The assessment would influence the valuation of the company and can guide negotiations regarding software-related aspects such as licensing rights, intellectual property, or potential remediation costs.

SBOMs can also aid in integration planning for post-acquisition or investment scenarios. By understanding the software components and dependencies of the target company, organizations can assess the compatibility and integration requirements with existing systems or technologies. As such, SBOMs assist in identifying potential conflicts, migration challenges, or opportunities for technology consolidation and optimization.



## Example

An investor can use SBOMs to compare the software supply chains of different target companies. This information can then be used to assess the security of each company and to make an informed decision about which company to invest in or acquire.



## Mission and Operational Readiness

### Getting Started

- Identify areas of technical debt
- Plan for upgrades to secure software versions
- Prioritize resources for remediation efforts to maximize impact

### Summary:

SBOMs can be used to make informed decisions about software procurement, development, and maintenance, such as determining which software components to use, how to mitigate risks, and where to invest resources.

### Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: n/a
- Malware: n/a
- Licensing: Yes
- Foreign Presence: Yes
- Attestation: n/a

**Common Tool Integration:** CMDBs • SAM • EDR • Vulnerability Scanners & Sensors • Supply Chain Risk Management Systems

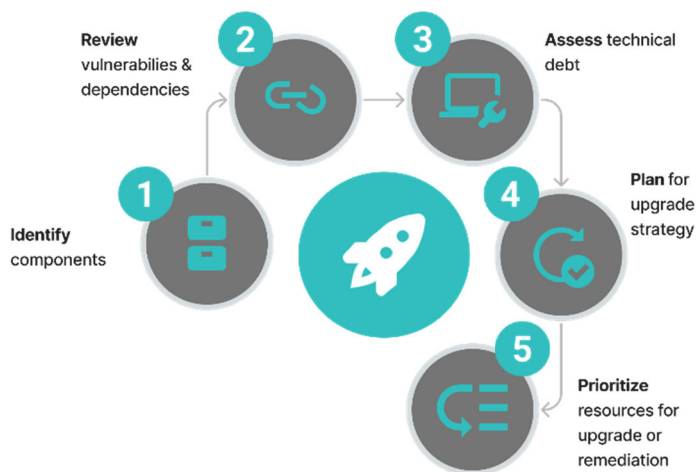
### Description

SBOMs provide visibility into software components and versions used in an application or system. This visibility can illuminate outdated components and technical debt, which refers to the accumulated consequences of suboptimal design or implementation choices. SBOM-related information can be used to assess compatibility requirements and to plan for the adoption of newer and more secure software versions or alternative components.

Having visibility into potential security vulnerabilities and dependencies helps in formulating risk management strategies, prioritizing resources for remediation efforts, and implementing effective security controls to prevent security incidents.

### Example

A utility board wishes to understand the relative risk hidden in the organization's software components versus the surface risk that is part of traditional vulnerability management programs.



## Efficient Internal Code Development

### Getting Started

- Identify internal teams that are producing software
- Inquire about current tooling
- Discuss opportunities to augment decision making and business case with stakeholders
- Establish governance for risk tolerance levels and time-to-fix

### Summary:

Large enterprises often have internal software development teams. Code reuse is common practice in modern software development, and these teams must have methods to ensure the code being used will lead to efficient and secure deliverables.

**Answers:** *Is my internal software being developed securely?*

### Relevant Risk Areas

- Vulnerability: Yes
- Dependency: Yes
- Integrity: Yes
- Malware: Yes
- Licensing: Yes
- Foreign Presence: Yes
- Attestation: Yes

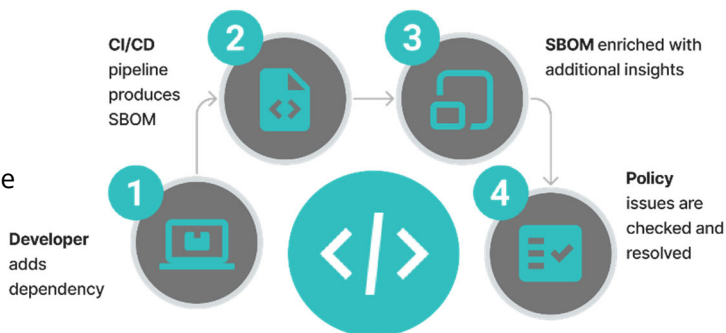
**Common Tool Integrations:** Developer Tooling • Continuous Integration / Continuous Development (CI/CD) pipeline tools • Software Composition Analysis (SCA) tools • Integrated Developer Environments (IDEs)

### Description

Benefits cited by National Technology and Information Administration (NTIA) publications detail how SBOMs can be used for internal software development to (i) reduce unplanned, unscheduled work, (ii) reduce code bloat, (iii) adequately understand dependencies within broader complex projects, (iv) know and comply with the license obligations, (v) monitor components for vulnerabilities, (vi) end-of-life (EOL), (vii) make code easier to review, (viii) compose a deny-list of components, and (ix) provide transparency to downstream users of the software.

### Example

A software developer analyzes SBOM to assess the presence of outdated or vulnerable components, identify areas of technical debt, and formulate a roadmap to address and reduce technical debt effectively.





# THE ROAD AHEAD



## Challenges to Achieving Use Cases



### Many Stakeholders, Little Awareness

Key challenges of using SBOMs include the need to operationalize the data. This includes obtaining, storing, managing, updating, and leveraging SBOMs for real insights. Fortress' SBOM Analysis provides actionable intelligence on SBOMs, allowing organizations to use the data to improve the security of their systems.

Additionally, when it comes to collecting and sharing SBOMS, there is a lack of common standards for data sharing. This can make it difficult to share SBOMs between different organizations in a repeatable, scalable method.

### Tool Maturity

There are many existing tools in for SBOMs. However, their quality can vary. Some factors to consider when judging the quality of a tool's output are as follows:

- SBOM adheres to standard formats (CycloneDX, SPDX)
- SBOM includes fields that help with identification:
  - Package identifier (Package URL, CPE, SWID, SWHID) Package hash (SHA-256, SHA1, etc.)
  - Vulnerability lookup identifiers (CVE, GHSA ID)
  - Version Control System location (GitHub, GitLab, Codeberg, BitBucket, etc.)
  - Digital signatures of the SBOM
  - Dependency relationship tree with more than one layer



## THE ROAD AHEAD

SBOMs can aid utilities in quickly responding to software supply chain attacks by giving them insight into the software components used in their operations. This visibility enables organizations to make informed decisions, maintain regulatory compliance, and strengthen their cybersecurity posture. Utilizing SBOM data with visualization tools and workflows optimizes their potential to improve overall security.

To address this challenge of providing a central inventory of software components for utility companies, several investor-owned utilities, including American Electric Power and Avangrid, partnered with Fortress to launch the North America Energy Supply Assurance Database (NAESAD). NAESAD securely aggregates SBOMs for every utility industry vendor. In close collaboration with forward-looking software providers, this repository will enable utilities to identify, triage, and remediate the most impactful and destructive risks.

## ABOUT THE AUTHORS



Ty Short is the Vice President of Product at Fortress Information Security. Short, while focused on product portfolio management, brings diverse executive experiences over a 20-year career to the team ranging from entrepreneurship, software development, systems engineering, to financial planning & analysis. Ty maintains an active CPA license, holds a master's in accounting, and is an alumnus of the Kellogg School of Management's Chief Product Officer program.



Bryan Cowan is the Product Owner on Fortress' solutions for Software Bills of Materials (SBOMs). His work focuses on software transparency and improving supply chain security using SBOMs and Vulnerability Exploitability eXchange (VEX), including ways to automate and to improve operational vulnerability response. Bryan joined Fortress after completing a master's thesis on the topic of SBOMs and medical devices. Bryan holds a master's in information systems security.



Fortress Information Security was founded in 2015 in Orlando, Florida with a mission to secure critical infrastructure sectors from supply chain cybersecurity risks.

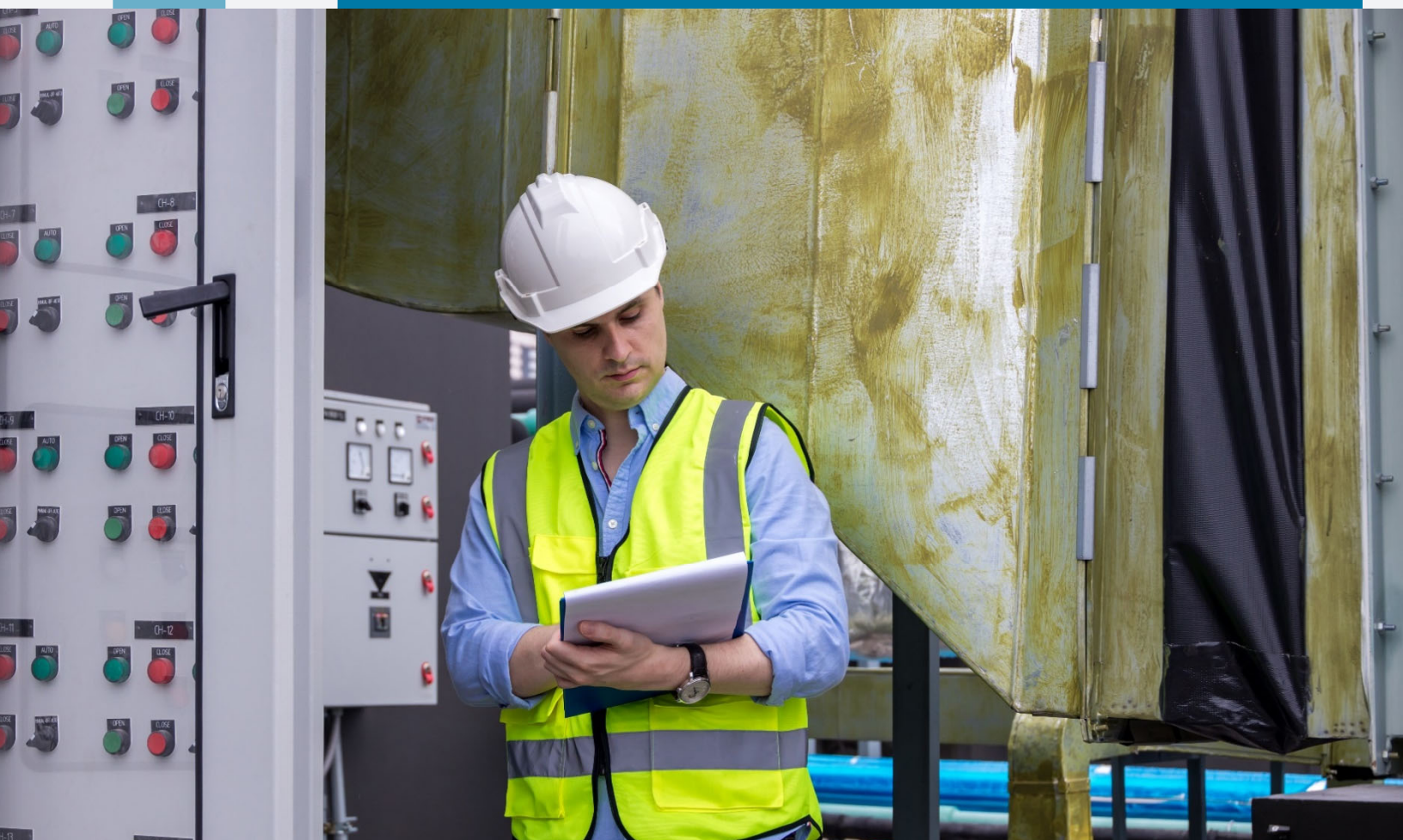
Fortress delivers solutions through its platform, data, and services. Key product offerings include vendor assessments, product (both software and hardware) assessments, vendor monitoring, product monitoring, and vulnerability management.

Fortress also hosts several industry data exchanges including the Asset to Vendor Network for vendor assessments and the North American Energy Software Assurance Database addressing software transparency (including SBOMs) and emerging risk areas.

Version 9.1 2023-08-08



# APPENDIX 1: CONTEXT FOR SBOM



## Introduction

Electric utilities are responsible for providing reliable and safe power to millions of customers. To achieve this, they must maintain a complex infrastructure of power generation, transmission, and distribution systems. One of the challenges facing utilities today is the need to effectively manage the security of their systems, particularly in the face of growing cyber threats. One new tool that can help utilities improve their security posture is the Software Bill of Materials (SBOM). SBOMs can help electric utilities improve their overall security posture by providing a detailed and centralized view of their software components and enabling them to identify and address vulnerabilities before they can be exploited by threat actors.

SBOMs provide a comprehensive inventory of all software components, enabling organizations to quickly identify vulnerabilities and track them to their origin. By having a complete and up-to-date understanding of their software ecosystem, organizations can make informed decisions on software updates and patches, reducing the risk of exploitation of known vulnerabilities.

SBOMs provide a listing of proprietary and open-source ingredients in software that run critical infrastructure technologies. SBOMs provide actionable information to purchasers so they can make informed decisions about software and help improve the security of applications. While many standards and guidelines require varying levels of software security, an effectively prepared and analyzed SBOM can be invaluable in meeting tomorrow's critical infrastructure application cybersecurity challenges.

To address this challenge of providing a central inventory of software components for utility companies, several investor-owned utilities, including American Electric Power and Avangrid, partnered with Fortress to launch the North America Energy Software Assurance Database (NAESAD). NAESAD will securely aggregate SBOMs for every utility industry vendor. In close collaboration with forward-looking software providers, the repository will enable utilities to identify, triage, and remediate the most impactful and destructive risks.

## APPENDIX 1

## The Threat

Software supply chain attacks are increasing in frequency, sophistication, and complexity. One notable example is the widely used component, Log4j, which contained a zero-day vulnerability and compromised the software supply chain. Vulnerabilities like Log4j can seriously impact an organization's overall security posture by potentially exposing sensitive data and systems to attackers. Compromised components can spread quickly throughout an organization's IT infrastructure and be used to launch more widespread attacks, leading to a significant breach.

Other examples of high-profile supply chain attacks include:

- The SolarWinds Orion attack, in which attackers compromised the build system of a network management system and inserted backdoor malware into software updates distributed to customers.
- The Codecov incident, in which attackers compromised a code testing tool used by companies like GoDaddy.
- The Royal Bank of Canada, in which sensitive information was exfiltrated.
- The PHP programming language attack, in which hackers compromised a server used to distribute the language and added a backdoor to the source code, making websites vulnerable to a complete takeover.

In addition, common trends such as an increasingly remote workforce, the use of open-source code sources, and shadow IT all leave organizations with a growing attack surface. These trends have increased the exposure to supply chain attacks as well as the likelihood of compromise.

While the NAESAD Asset Vulnerability Management system may not qualify for the CRISP1 program, participation in the NAESAD would enable utilities to monitor IT or OT systems through the Fortress software active monitoring program. As new vulnerabilities are identified, our system will:

- Proactively identify new vulnerabilities and zero-day threats.
- Identify software or software components that have detected malware or vulnerabilities.
- Coordinate remediation across industry peers to ensure supplier cooperation.
- Incident Management services to immediately identify exposed software or software components (SBOMs) that may be vulnerable to an active incident or vulnerability notice.

**Fortress can help utilities prepare justification for how the NAESAD and Asset Vulnerability Management solutions can be prequalified for FERC incentives.**

## What is an SBOM?

An SBOM, or Software Bill of Materials, is an inventory of the components used in a software product. It includes important information such as the component supplier name, component name and version, unique component identifiers, and information about the relationships between components.

Software developers often use a mix of software components to speed up the development process. As a result, a typical software product is often composed of a combination of proprietary code along with commercial and open-source components. The commercial and open-source components can have hundreds or thousands of subcomponents, and the relationships between them are known as “dependencies.”





## How are SBOMs obtained?

Ideally, software vendors will provide SBOMs upon request, as they are in the best position to provide accurate “build” SBOMs (created during the build process) and “analyzed” SBOMs (from resulting binaries). Many large software suppliers are now producing SBOMs for their own internal risk management functions. Furthermore, producing independently analyzed SBOMs using binary or firmware analysis tools helps to ensure that what was provided by the supplier matches the software in use, or in cases of legacy products, or when a vendor is unable or unwilling to provide an SBOM.

If software vendors are unable or unwilling to provide SBOMs, Fortress has the capability to interrogate the software using a variety of both commercial and internally developed tools, on most files and firmware images. These tools and subsequent analysis of the results provide visibility into the individual libraries and dependencies used when creating the application to better assess any risks presented by bringing the software into a production environment.

## Why are SBOMs Important for Electric Utilities?

Electric utilities rely heavily on a complex network of systems to manage and control the generation, transmission, and distribution of electricity. These systems are critical to the operation of the electric grid, and any disruption or compromise can have severe consequences. By creating and maintaining SBOMs for critical systems, utilities can gain a better understanding of the software components used in their operations and can use this information to contextualize potential security risks to their environment.

An SBOM does not directly offer security, but it does offer a comprehensive view of the software components used in a software package. This helps organizations maintain an accurate inventory of their assets, enabling them to analyze vulnerabilities and prioritize risks more effectively. As a result, their overall security posture is improved. Traditional application security involved waiting for patches for entire products without the perspective that an SBOM provides at the component level. With a better understanding of the software components, effective mitigation and more informed risk acceptance will allow for enhanced risk-based decision making.



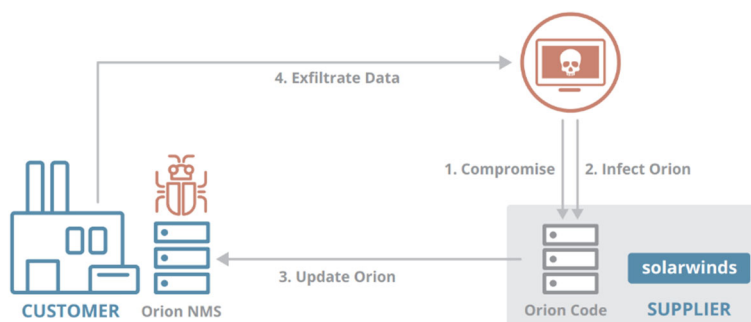
## APPENDIX 2: SUPPLY CHAIN ATTACK EXAMPLES





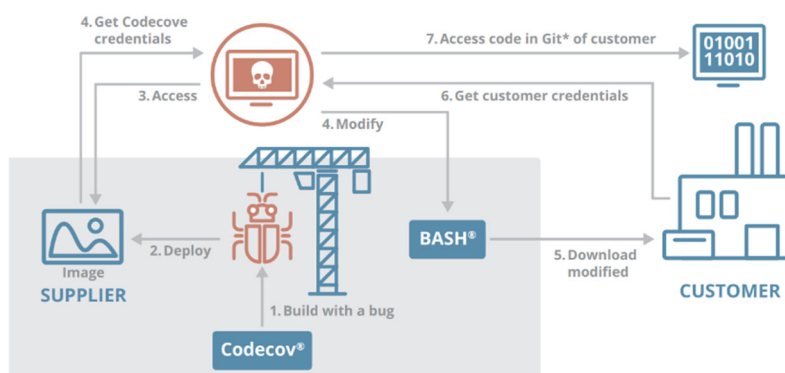
## SolarWinds Orion

In the SolarWinds Orion attack, attackers used a combination of techniques to access SolarWinds' Orion IT monitoring and management software. The attackers modified Orion's code and took advantage of the trusted relationship between the company and its customers to distribute and update customer applications with malware. The malware was used to tap into the final target: SolarWinds' customers data.<sup>15</sup>



## Codecov

In the Codecov incident, attackers were able to extract a credential from a Codecov Docker image due to errors in how the images were created. Using these credentials, the attackers compromised a Bash uploader script used by customers. Once this script was executed by a customer, the script would send all CI environment variables to the attacker. Customers reported the attackers were able to access their source code and other sensitive information.<sup>16</sup>

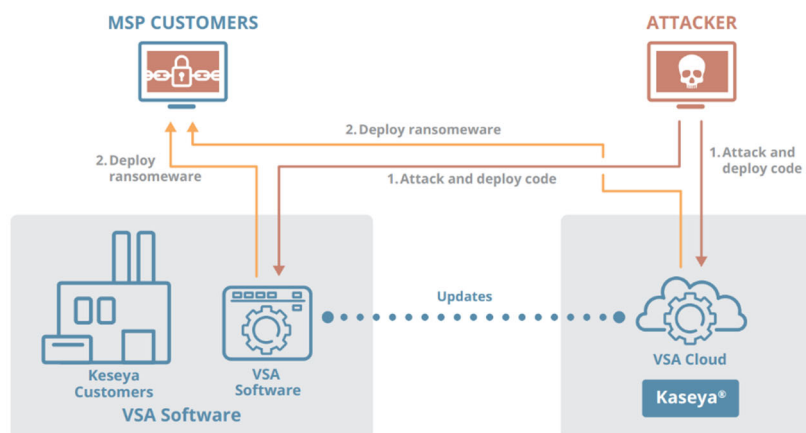


<sup>15</sup>ENISA. Threat Landscape for Supply Chain Attacks, p. 45. <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>


<sup>16</sup> ENISA. Threat Landscape for Supply Chain Attacks, p. 32. <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

## Kaseya

Kaseya offers Virtual System/Server Administrator (VSA) software and provides cloud servers. VSA software can be used on premises or cloud servers. Attackers used a zero-day vulnerability to remotely execute commands on VSA cloud servers and then remotely sent out updates that contained malicious code to VSA servers. This code deployed ransomware on some 1,500 end customers and 30 Managed Service Providers (MSPs).<sup>17</sup>



<sup>17</sup> ENISA. Threat Landscape for Supply Chain Attacks, p. 19. <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>



## APPENDIX 3: USE CASE QUICK REFERENCE



Use Case	Summary	Example
<b>Incident Response</b>	Traditional incident response involves waiting for patches for entire products without the perspective that an SBOM provides at the component level. With a better understanding of the components, effective prioritization and mitigation as new vulnerabilities appear.	Significant disruption was caused when critical severity vulnerabilities were discovered in Apache Log4j in December 2021, a popular Java logging utility. Organizations expended value time and resources to discover if they were affected. Using SBOMs as an up-to-date inventory, an incident response team can proactively identify which assets are affected by new vulnerabilities, prioritize mitigation for critical assets, and reach out to vendors whose products are impacted.
<b>Third-Party Risk Mgmt.</b>	SBOMs can assist in assessing the security posture of third-party software suppliers and vendors. By requesting SBOMs from suppliers and reviewing the components and vulnerabilities present, organizations can make informed decisions about the security and trustworthiness of the software they integrate into their systems.	A Utility company can use an SBOM to identify all third-party software components used in its industrial control systems. This information can then be used to assess the cybersecurity risks associated with these components and implement appropriate security controls.
<b>Architecture Review</b>	SBOMs provide a comprehensive inventory of the software components A financial services company can use an SBOM to identify all third-party and dependencies used in an application. By analyzing the SBOM, organizations can review product policy concerns before installation, and ensure that the architecture is secure and reliable.	A financial services company can use an SBOM to identify all third-party software components used in its trading platform. This information can then be used to enforce IT policies against using insecure versions of common components, such as Apache Struts v2.3.5.
<b>Vulnerability Management</b>	With SBOMs in hand, vulnerability management tools and platforms can compare the listed components against known vulnerability databases. This allows organizations to prioritize vulnerabilities based on their severity and potential impact on the application's security.	A security analyst can use an SBOM to identify all the software components used in a network. This information can then be used to search for known vulnerabilities in those components and to prioritize remediation efforts.
<b>Security Preview</b>	SBOMs can be used during the software vendor selection process to evaluate the risks associated with software components. Reviewing the SBOM can provide utilities with insights into potential risks posed by software components, such as the use of outdated software versions, software with known vulnerabilities, or components with a history of security incidents.	A healthcare organization can use an SBOM to identify the open-source software components used in a proposed electronic health record (EHR) system. This information can then be used to assess the security risks associated with these components.
<b>Contract Conditions</b>	SBOMs provide valuable information that can inform the decision-making process during procurement. Organizations can use the SBOMs to compare different software options, assess their security and risks, and make informed choices. Additionally, the	A healthcare organization can use an SBOM to identify all open-source software components used in newly proposed electronic health record (EHR) systems. The chosen solution was found to include a few high-severity vulnerabilities, so a remediation timeline was

Use Case	Summary	Example
	SBOM information can be used for negotiation purposes, ensuring that security requirements, vulnerability management practices, and compliance obligations are adequately addressed in vendor contracts.	included in the purchase agreement.
<b>Licensing Compliance</b>	Ensure that internally developed and procured software are free of restrictions or obligations. By providing visibility into the software supply chain and the licenses that govern it, SBOMs can help organizations to identify and address any potential compliance issues before they cause problems.	A manufacturer can use SBOMs to track the licenses of components in software from open-source libraries, third-party vendors, internally developed software, and partner companies. By proactively checking compliance with license terms, they can avoid costly, and time-consuming litigation.
<b>Vulnerability Mandates</b>	Transportation Security Administration (TSA) provides several cybersecurity requirements, and North American Electric Reliability Corporation (NERC) recommends SBOMs as useful tool for supply chain provenance and vendor risk management.	An investor-owned utility (IOU) requires vendors to provide SBOM as part of a procurement process. Using the component information helps identify all known vulnerabilities. Then they prioritize patch requests to vendors based on the asset's criticality. After patches are provided, they receive an updated SBOM to confirm the component updates resolved the vulnerability.
<b>SBOM Collection</b>	Customers and regulators are looking for transparency so they can better secure the software that powers their everyday operations. Scalable and secure sharing methods encourage sharing, and collection of SBOMs and provide actionable information for the environment.	An automaker contracts with an SBOM services provider to collect SBOMs on products from Tier 1 supplier. The service provider aggregates SBOMs from vendors via an authenticated API connection and receives permission from the Tier 1 supplier before furnishing the document to their mutual customer.
<b>Investing</b>	SBOM can be used in due diligence and decision-making support of investing or mergers and acquisitions (M&A) use cases to assess the software-related risks and opportunities associated with target companies.	An investor can use SBOMs to compare the software supply chains of different target companies. This information can then be used to assess the security of each company and to make an informed decision about which company to invest in or acquire.
<b>Mission &amp; Operational Readiness</b>	SBOMs can be used to make informed decisions about software procurement, development, and maintenance, such as which software components to use, how to mitigate risks, and where to invest resources.	A software developer analyzes SBOM to assess the presence of outdated or vulnerable components, identify areas of technical debt, and formulate a roadmap to address and reduce technical debt effectively.



## APPENDIX 4: REGULATIONS AND INDUSTRY GUIDELINES



## Drivers of Supply Chain Cybersecurity Regulations

Disruption driven by technology is inevitable. Today, we deal with an upsurge in attention towards supply chain cybersecurity. The driving forces behind this shift include:

### **Accelerated Digital Transformation**

- The pervasive incorporation of Internet of Things (IoT) devices, autonomous vehicles and systems, generative artificial intelligence, remote workforces in the post- COVID-19 era, private cellular networks, connected personal health devices, among others, has significantly amplified our reliance on software. The rapid expansion of these digital facets is expected to continue, further heightening our dependency.

### **Emergence of Sophisticated Cyber Threats**

- Cybercrime syndicates have evolved into structured businesses providing services like 'Access as a Service' and 'Ransomware as a Service'. This shift indicates an escalating sophistication in threat vectors. Furthermore, foreign adversaries, including but not limited to China, Russia, and North Korea, are reportedly engaging in deliberate efforts to destabilize our digital infrastructure, underscoring the necessity for robust cybersecurity measures.

### **Lack of Transparency in Software Supply Chains**

- The responsibility for cybersecurity has traditionally been shouldered by the end user, with minimal obligations placed on manufacturers to ensure supply chain transparency or guarantee security. This practice lags behind conventional models where manufacturers offer warranties for hardware failures. A paradigm shift is needed to align the cybersecurity standards with established norms, thereby reinforcing the integrity of our digital ecosystems.

## **Regulatory Response**

The White House has set the tone for cybersecurity strategy, and other agencies such as the Cybersecurity and Infrastructure Security Agency (CISA), North American Electric Reliability Corporation (NERC), Office of Management and Budget (OMB), and the Food and Drug Administration (FDA) have all rallied around this strategy. Associations in the energy sector such as the Edison Electric Institute (EEI) and the North American Transmission Forum (NATF) have also taken on recommendations for best practices.



## Biden-Harris 2023 Cybersecurity Strategy

Announced on March 2, 2023, the Biden-Harris 2023 Cybersecurity Strategy<sup>18</sup> identified two “fundamental shifts” in US cybersecurity strategy: (1) shift the burden of cybersecurity to those most capable, and (2) realign incentives for long term investments in cybersecurity.

Here are some of the key initiatives outlined in the strategy:

- Investing \$10 billion in cybersecurity infrastructure over the next five years.
- Creating a new Cybersecurity and Infrastructure Security Agency (CISA) directorate to focus on critical infrastructure protection.
- Requiring federal agencies to adopt a zero-trust security model.
- Increasing public awareness of cybersecurity risks.
- Working with allies and partners to share information and develop joint responses to cyber-attacks.
- Developing new technologies and capabilities to defend against cyber-attacks and to conduct offensive cyber operations.
- Holding perpetrators of cyber-attacks accountable.

This strategy is setting the tone for organizations such as CISA, FDA, DHS, DOE, and other agencies that cybersecurity (including software supply chain security) should be handled as a top priority.

---

## Executive Order 14028

The following is an excerpt from GSA describing EO 14028.<sup>19</sup>

Executive Order (EO) 14028 – “Improving the Nation’s Cybersecurity” (issued May 12, 2021) requires agencies to enhance cybersecurity and software supply chain integrity.

### Summary of EO 14028 requirements:

- Requires service providers to share cyber incident and threat information that could impact Government networks.
- Moves the Federal government to secure cloud services, zero-trust architecture, and mandates deployment of multifactor authentication and encryption within a specific time period.

---

<sup>18</sup> White House. Biden-Harris Administration Announces National Cybersecurity Strategy.

<https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>

<sup>19</sup> GSA. Executive Order 14028: Improving the Nation's Cybersecurity. <https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028>

- Establishes baseline security standards for development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available.
- Establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads, that may convene following a significant cyber incident to analyze what happened and make recommendations for improving cybersecurity.
- Creates a standardized playbook and set of definitions for cyber incident response by Federal departments and agencies.
- Improves the ability to detect malicious cyber activity on Federal networks by enabling a government-wide endpoint detection and response system and improved information sharing within the Federal government.
- Creates cybersecurity event log requirements for Federal departments and agencies.
- Requires amendments to the FAR to align with requirements in the EO.

### What contractors can expect<sup>20</sup>

- Modification of contract language to reflect new guidance from NIST and CISA. If your company cannot accept the modification, you will not be able to sell to the Federal government.
- GSA will keep you informed, communicating with you regarding all major developments.
- Future updates to the Federal Acquisition Regulation (FAR).

## OMB-22-18

Executive Order (EO) 14028, Improving the Nation's Cybersecurity (May 12, 2021), focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs agencies to take a variety of actions that "enhance the security of the software supply chain." In accordance with the EO, the National Institute of Standards and Technology (NIST) has released the NIST Secure Software Development Framework (SSDF), SP 800-218, and the NIST Software Supply Chain Security Guidance (hereinafter, referred to collectively as "NIST Guidance"). OMB Memorandum M-22- 18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M- 22-18) (Sept. 14, 2022), requires agencies to comply with that NIST Guidance. Pursuant to M-22-18, agencies must only use software that is provided by software producers who can attest to complying with Government-specified minimum secure software development practices.

<sup>20</sup> U.S. President. "Improving the Nation's Cybersecurity". <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>

### **The memorandum requires agencies to:**<sup>21</sup>

- Inventory all software used by their employees.
- Develop a process to communicate the memorandum's requirements to software producers.
- Collect attestation letters from software producers.
- Implement certain security practices for software development, including:
  - Using secure coding practices
  - Conducting security testing
  - Managing software changes
  - Protecting software from unauthorized access, use, disclosure, disruption, modification, or destruction

The memorandum also provides guidance on how agencies can implement the required security practices.

The memorandum is an important step in improving the security of the federal government's software supply chain. By implementing the requirements of the memorandum, agencies can help to protect their systems and data from malicious actors.

---

## **OMB-23-16**

OMB-23-16 memorandum updates M-22-18 Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, which required agencies to implement certain security practices for software development.

### **The update makes two changes:**<sup>22</sup>

- It allows agencies to continue using software that does not meet all required security practices, if the software producer has a plan in place to mitigate the risks.
- It clarifies that agencies are responsible for ensuring that all software used by their employees meets the required security practices, even if the software is not developed or maintained by the agency.

The memorandum also provides guidance on how agencies can implement the updated requirements. Here are some of the key points of the memorandum:

---

<sup>21</sup> OMB. M-22-18. <https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf>

<sup>22</sup> OMB. M-23-16. <https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf>

- Agencies must inventory all software used by their employees within 90 days of the memorandum's publication.
- Agencies must develop a process to communicate the memorandum's requirements to software producers within 120 days of the memorandum's publication.
- **Agencies must collect attestation letters from software producers within 270 days of the memorandum's publication.**
- Agencies may continue using software that does not meet all the required security practices if the software producer has a plan in place to mitigate the risks.
- Agencies are responsible for ensuring that all software used by their employees meets the required security practices, even if the software is not developed or maintained by the agency.

The memorandum is an important step in improving the security of the federal government's software supply chain. By implementing the requirements of the memorandum, agencies can help to protect their systems and data from malicious actors.

---

## EU Medical Device Regulation

The EU Medical Device Regulation (EU MDR) requires manufacturers of medical devices to provide a software bill of materials (SBOM) to notified bodies as part of the conformity assessment process.

The SBOM must include information about the following:

- The identity and version of each software component used in the medical device
- The source of each software component
- The license under which each software component is used
- Any known vulnerabilities in each software component

The EU MDR also requires manufacturers to keep the SBOM up to date throughout the life cycle of the medical device. This means that manufacturers must update the SBOM whenever they make changes to the software components used in the medical device.

---

## FDA Requirements

The Consolidated Appropriations Act, 2023, which was passed by Congress on December 23, 2022, and signed into law by President Biden on December 29, 2022, includes a provision that requires medical device manufacturers to provide a software bill of materials (SBOM) for medical devices that contain software, may connect to the internet, or may be exposed to cyber threats. The SBOM must

include information about the software components used in the device, including the name, version, and supplier of each component.<sup>23</sup>

As a result of this legislation, the Food and Drug Administration (FDA) will be requiring that SBOMs be submitted to it as part of the pre-market submission process for medical devices classified as “cyber devices” to encourage vendors to make their devices secure by design in the healthcare industry. Medical devices are unique in that they can be implanted in patients and monitor or regulate bodily functions. Security issues in a medical device can directly impact the lives of patients.

In March of 2023, the FDA issued guidance on a “Refuse to Accept Policy” for medical devices, which takes effect on October 1st, 2023. In addition to requiring pre-market submission for medical devices to include plans for vulnerability disclosure and patching, **this policy requires an SBOM to be submitted** as part of the application. A medical device maker must provide an SBOM for devices which qualify as a “cyber device” and are still recommended for non-cyber devices. The SBOM is to include a listing of commercial, open-source, and off-the-shelf software components, in industry recognized machine-readable formats, for example, CycloneDX and SPDS. The refusal to accept policy means that **any submission to the FDA for approval on a new medical device will be automatically refused if an SBOM is not provided**. The agency’s eSTAR system for pre-market submissions is being programmed to reject if an SBOM is not included. Starting in October 2023, SBOMs are a must for many medical device manufacturers.

---

## Secure by Design, Secure by Default by CISA

CISA issued guidance for Secure by Design and Secure by Default on April 13, 2023.<sup>24</sup> The section discussing Secure by Design<sup>25</sup> includes a non-exhaustive list of best practices:

- Memory safe programming languages (SSDF PW.6.1)
- Secure Hardware Foundation
- **Secure Software Components** (SSDF PW 4.1): Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks) from verified commercial, open source, and other third-party developers to ensure robust security in consumer software products
- Web template frameworks (SSDF PW.5.1)
- Parameterized queries (SSDF PW 5.1)
- Static and dynamic application security testing (SAST/DAST) (SSDF PW.7.2, PW.8.2)
- Code review (SSDF PW.7.1, PW.7.2)

---

<sup>23</sup> U.S. Congress. H.R.2617 - Consolidated Appropriations Act, 2023. <https://www.congress.gov/bills/117th-congress/house-bill/2617/text>

<sup>24</sup> CISA. U.S. and International Partners Publish Secure-by-Design and -Default Principles and Approaches. <https://www.cisa.gov/news-events/news/us-and-international-partners-publish-secure-design-and-default-principles-and-approaches>

<sup>25</sup> CISA. Security-by-Design and -Default. <https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default>

- **Software Bill of Materials (SBOM) (SSDF PS.3.2, PW.4.1):** Incorporate the creation of SBOM to provide visibility into the set of software that goes into products
- Vulnerability disclosure programs (SSDF RV.1.3)
- CVE completeness
- Defense-in-Depth
- Satisfy Cyber Performance Goals (CPGs)



## Utility Regulatory Landscape

As of the time of this publication, there are no explicit requirements to collect or utilize SBOMs from utility regulatory bodies such as NERC. However, there are many precedents and guidelines that point to the use of SBOMs as well as several anticipated authoritative documents on the topic.

### Model Procurement Contract Language by EEI

The Edison Electric Institute (EEI) is an association that represents U.S. investor-owned electric companies. EEI provides advocacy, industry data, networking and collaboration, education and training, public relations, standards development, research, and innovation. EEI publishes contract language guidelines in its Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk (MPCL), which is presently on version 3.0, last updated October 2022. The MPCL introduced the SBOM requirement in May 2020 in response to the NERC CIP-013-1 Cyber Security—Supply Chain Risk Management standard which became effective on October 1, 2020. Addressing CIP-013's R1.2.5 "Verification of software integrity and authenticity..." the MPCL states for "Hardware, Firmware, Software, and Patch Integrity and Authenticity" in



section (e): Contractor shall provide a software bill of materials for procured (including licensed) products consisting of a list of components and associated metadata that make up a component.<sup>26</sup>

## NERC Security Guideline – Vendor Risk Management Lifecycle

As a NERC Security Guideline, “Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.”<sup>27</sup>

“Most supply chain cyber security risks originate with vendors, so they are the most important component of an entity’s Bulk Electric System (BES) supply chain cyber security risk management plan. This security guideline describes how an entity can identify, assess, and mitigate vendor cyber security risks as well as document their vendor risk management program.”

The guide provides specific guidance on using SBOMs during the Request for Proposal (RFP) process for vendor and product selection.

One risk mitigation measure is to request in the RFP that the vendor provide a software bill of materials (SBOM) listing all components of their software and/or firmware that were developed by third parties – whether proprietary or open source.

An SBOM allows the entity to identify components and hold the vendor accountable for providing patches for vulnerabilities identified in the components that are exploitable in the product itself. Note that it is reasonable to expect that a supplier will require an NDA to be in place before they will provide SBOMs to a customer.

## NERC Security Guideline – Supply Chain Provenance

As a NERC Security Guideline, “Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.”<sup>28</sup>

- Require vendors to provide a bill of materials:

---

<sup>26</sup> Edison Electric Institute. Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk.

<https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Model--Procurement-Contract.pdf>

<sup>27</sup> NERC. Security Guideline, Vendor Risk Management Lifecycle.

[https://www.nerc.com/comm/RSTC\\_Reliability\\_Guidelines/Security\\_Guideline-Vendor\\_Risk\\_Management\\_Lifecycle.pdf](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf)

<sup>28</sup> NERC. Security Guideline, Supply Chain Provenance.

[https://www.nerc.com/comm/RSTC\\_Reliability\\_Guidelines/Security\\_Guideline-Supply%20Chain%20Provenance.pdf](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Supply%20Chain%20Provenance.pdf)

- Every software or firmware supplier and every supplier of intelligent devices to an organization should be able to or have a plan to provide a bill of materials that includes a hardware bill of materials (HBOM), a software bill of materials (SBOM), or both.
- The SBOM should be generated for every configurable option for that product and hardware revision, and it should be re-issued for new hardware profiles or any time a hardware component changes within the manufacturing process. Every HBOM should contain the model and version number for the product and a reference to the associated SBOM if applicable.
- The SBOM should be re-issued whenever the software changes, including upon application of an update or patch to a product in use at the organization. An SBOM should always contain a unique version number for the product, and every version number should correspond to a unique SBOM. All bills of material should contain a unique time stamp, a means of verifying its authenticity through cryptographic methods, and a unique version number. Further information about SBOMs is available from the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration.

---

## AUVSI - Green Uncrewed Aircraft System (UAS)

AUVSI (autonomous and uncrewed vehicle systems international), in partnership with Fortress Information Security, created the first recognized cybersecurity certification for drones, maritime vehicles, and land autonomous systems. To become certified, applicants must submit and maintain current software bills of materials and hardware bills of materials.<sup>29</sup>

---

## Product Sourcing Guide – NERC SCWG

The NERC Supply Chain Working group is working on a guide that will create a technology standard like what AUVSI has done in the drone space for consideration prior to making a purchase. It is expected that this will be released before the end of 2023 and will contain strong recommendations for collecting SBOMs as part of the sourcing process.

---

<sup>29</sup> AUVSI. AUVSI and Fortress Information Security Team to Develop Industry-Wide Cybersecurity Risk-Based Framework for Uncrewed Vehicles. <https://www.auvsi.org/auvsi-and-fortress-information-security-team-develop-industry-wide-cybersecurity-risk-based>

## ISO 14971

ISO 14971 Medical devices – Application of Risk Management to Medical Devices is a risk management standard specifically designed for medical devices. While ISO 14971 does not directly relate to software bills of materials (SBOMs), it provides a framework for conducting risk management activities, including risk assessment and risk control, which can be applicable to the development and use of software in medical devices.

When it comes to software development and integration within medical devices, including SBOMs can be beneficial for risk management practices in accordance with ISO 14971:

1. **Risk identification:** ISO 14971 emphasizes the identification of potential hazards and risks associated with medical devices. In the context of software development, including SBOMs can aid in identifying potential risks introduced by software components, such as known vulnerabilities or dependencies on unsupported software versions.
2. **Risk analysis:** ISO 14971 guides the analysis and evaluation of identified risks to determine their significance and impact on patient safety. SBOMs can assist in the risk analysis process by providing information about software components, their known vulnerabilities, and associated risk levels. This helps in assessing the potential impact of software-related risks on the overall risk profile of the medical device.
3. **Risk control:** ISO 14971 outlines risk control measures to mitigate identified risks. SBOMs can be used to implement risk control strategies by enabling the identification of specific software components that pose significant risks. Organizations can then take appropriate actions, such as applying patches, updating software versions, or substituting components, to reduce or eliminate the identified risks.
4. **Post-market surveillance:** ISO 14971 emphasizes the importance of post-market surveillance to monitor and address potential risks associated with medical devices throughout their lifecycle. SBOMs can facilitate post-market surveillance efforts by providing visibility into the software components used in the device. This enables organizations to track and manage software-related risks and vulnerabilities even after the device is in use.



## Operationalizing SBOM – NATF

The North American Transmission Forum (NATF), the Department of Energy (DOE), the Idaho National Laboratory (INL), the Department of Homeland Security (DHS), and Fortres Information Security, are working to create an SBOM guide that is endorsed by NERC. This guide will serve as another point of reference for business justification and uses for practical SBOM implementation into existing risk management processes.

## SBOM Regulatory Summary

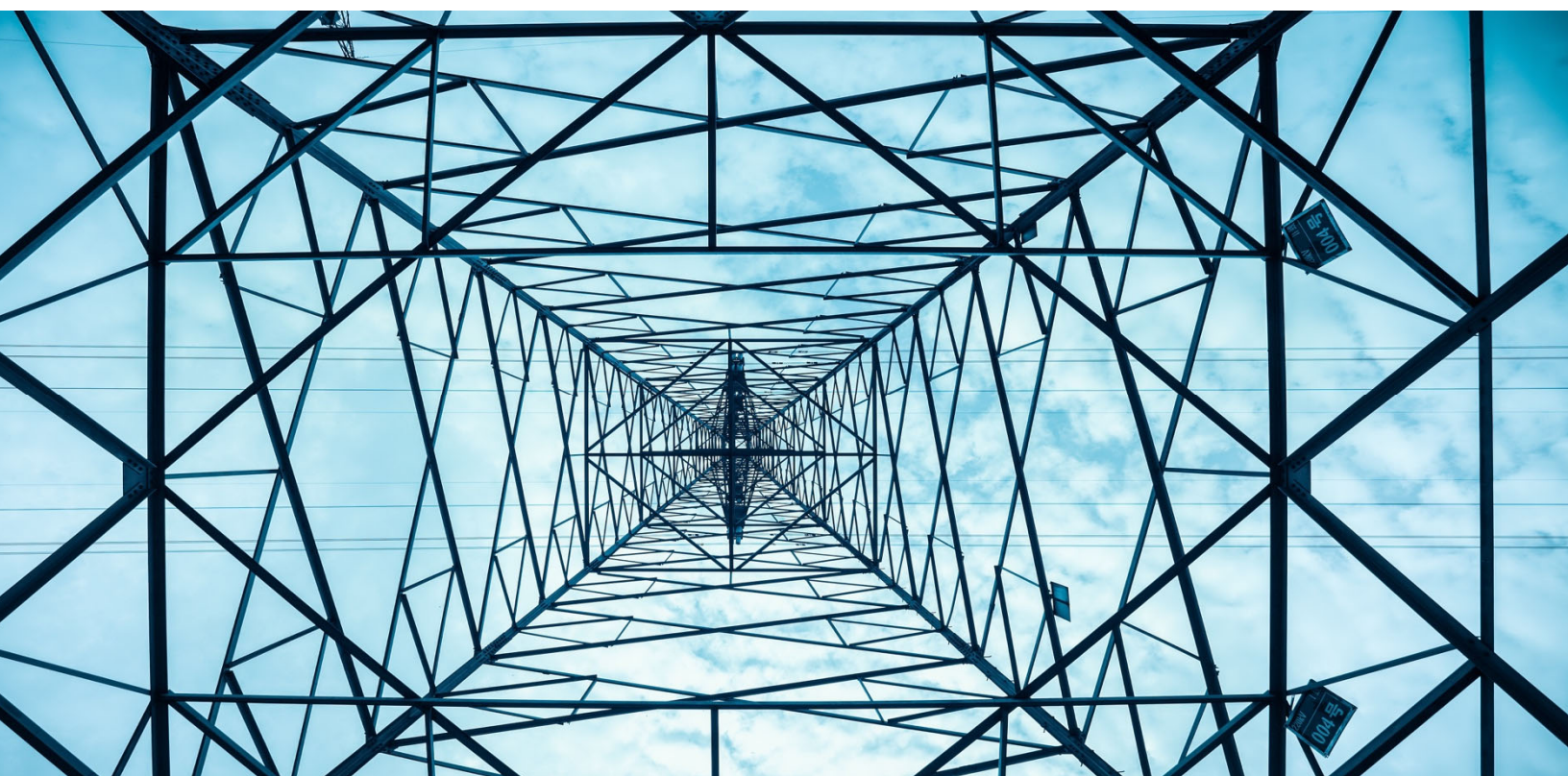
This table can be used by professionals seeking to raise awareness of the importance and inevitability of using SBOMs as a risk management tool.

Regulation	Description
FDA Refuse to Accept Policy	Medical device manufacturers will be required to submit an SBOM for new medical cyber devices starting October 1, 2023.
EO 14028 and related memos OMB-22-18, OMB-23-16	Requirement of federally owned entities to collect software attestations for all software used. Implementation depends on approval timelines which are expected in early 2024. This directly impacts certain utilities such as TVA, SWPA, WAPA, and Bonneville.
NERC Security Guideline – Vendor Risk Management Lifecycle	“One risk mitigation measure is to request in the RFP that the vendor provide a software bill of materials (SBOM) listing all components of their software and/or firmware that were developed by third parties – whether proprietary or open source.” Update was made in Mar 2023.
NERC Security Guideline – Supply Chain Provenance	“Every software or firmware supplier and every supplier of intelligent devices to an organization should be able to or have a plan to provide a bill of materials that includes a hardware bill of materials (HBOM), a software bill of materials (SBOM), or both.” Update was made in Mar 2023.
Model Procurement Contract Language by EEI	Requiring SBOMs from suppliers is a best practice. Language has been in effect since 2020.
Anticipated NERC SCWG Product Sourcing Guide	NERC Supply Chain Working Group plans to issue a sourcing guide in 2023 that will further support software supply chain transparency through the collection and use of SBOMs.
Anticipated NATF Operationalizing SBOM	A joint initiative between NATF, DOE, DHS, INL, Fortress Information Security, and others, to provide further guidance on practical SBOM implementations. This is expected to be released in 2023.





## **APPENDIX 5: SUMMARY OF INCENTIVES FOR ADVANCED CYBERSECURITY**





### **Rule Summary: Incentives for Advanced Cybersecurity Investment<sup>30</sup>**

On April 21, 2023, the Department of Energy (DOE), under the aegis of the Federal Energy Regulatory Commission (FERC), issued its “Incentives for Advanced Cybersecurity Investment” (Docket No. RM22-19-000; Order No. 893). The rule includes revisions to prior regulations aimed at providing incentive-based rate treatment for transmitting electric energy in interstate commerce, and the sale of electric energy by utilities wholesale in interstate commerce.

The new rule’s objective is intended to benefit consumers by encouraging investments by utilities in Advanced Cybersecurity Technology and their participation in cybersecurity threat information sharing programs, as directed by the Infrastructure Investment and Jobs Act of 2021.

### **Focus on Voluntary Cybersecurity Investments in Advanced Cybersecurity Technology**

The final rule by FERC revised section 219A of the Federal Power Act (FPA) to establish rules for incentive-based rate treatment for certain voluntary cybersecurity investments by utilities. The newly established rules allow for incentive-based rate treatment and cost recovery for these investments by utilities that focus on voluntary cybersecurity investments in Advanced Cybersecurity Technology, such as solutions that enhance their security posture and better protect consumers by improving their ability to protect against, detect, respond to, or recover from a cybersecurity threat. Importantly, it extends incentive-based rate treatment to utilities that participate in cybersecurity threat information sharing programs and invest in advanced threat monitoring solutions.

The new incentive-based rules support implementation of the directives under the Infrastructure Investment and Jobs Act of 2021 (IIJA), signed into law in November 2021, calling for FERC to revise its regulations to establish the above rate treatments as part of efforts to enhance the security posture of the Bulk-Power System.

As part of its mandate, the rule establishes two eligibility criteria, requiring that each cybersecurity investment:

1. materially improves cybersecurity through either Advanced Cybersecurity Technology or participation in a cybersecurity threat information sharing program; and
2. is not already mandated by the Reliability Standards, or otherwise mandated by local, state, or federal law, decision, or directive; otherwise legally mandated; or an action taken in response to a federal or state agency merger condition, consent decree from federal or state

---

<sup>30</sup> FERC. E-1-RM22-19-000, “Incentives for Advanced Cybersecurity Investment”. <https://www.ferc.gov/media/e-1-rm22-19-000-0>.


agency, or settlement agreement that resolves a dispute between a utility and a public or private party. In establishing a regulatory framework for utilities to request incentive-based rate treatment for certain voluntary cybersecurity investments, the Commission details specific criteria defining each of the operational elements of the rule. These range from defining cybersecurity investments, establishing requirements for utility eligibility for rate incentives based on cybersecurity investments, to a detailed discussion of cybersecurity investment rate incentives.

The Commission also adopted a model to evaluate cybersecurity investments, which includes using a list of pre-qualified expenditures (PQ List) that are determined by the Commission to be eligible for incentives. Any cybersecurity investment on the PQ List would qualify under a “rebuttable presumption of eligibility” for an incentive, which will presumably expedite the review and approval process for these activities. The list will be posted on the Commission’s public website and a process for managing and updating that list will be developed to ensure it can keep evolving and keep pace with the dynamic threat landscape.

The Commission also adopted an option to file to receive incentive-based rate treatment for activities not on the PQ list. These will be evaluated on a case-by-case basis under the framework set forth in the rule and other applicable general rate review criteria.

In its full sweep, the rule constitutes a big step forward to incentivize enhanced cybersecurity investments in our power grid and sets forth a new framework designed to accomplish these objectives:

1. Identify the utilities permitted to request incentive-based rate treatment for cybersecurity investments.
2. Establish criteria by which the Commission can determine whether a cybersecurity investment is eligible to receive an incentive-based rate treatment.
3. Discuss the approaches that a utility may use to demonstrate that a cybersecurity investment satisfies the eligibility criteria.
4. Explain the types of incentive-based rate treatments available for qualifying cybersecurity investments.
5. Set limits on the duration of the incentive-based rate treatment.
6. Describe what utilities must include in their applications for incentive-based rate treatment for cybersecurity investments.
7. Enable cybersecurity investment cost to be part of the utility’s rate base such that a return can be earned on the unamortized portion of the investment; and
8. Establish the annual reporting requirements for utilities that receive incentive-based rate treatment for their cybersecurity investments.



## **APPENDIX 6: BUILDING A BUSINESS CASE**



## Introduction

It is said that finance is the language of business. Further, great ideas – even those that benefit national security – often must be justified with numbers, showing that one course of action will yield greater results than another. A simple example of this is, say, a cybersecurity investment of \$100 is being considered and is expected to yield a probability-weighted savings from breaches of \$110 (\$10 more than the investment); the savings exceeds the investment, and thus a favorable financial business case has been made.

This section offers ideas on how a business leader may quantify the benefits of an investment in SBOM solutions with greater savings coming from greater adoption among intended use cases. These savings should be combined with additional benefits from capital treatment and financial incentives covered elsewhere in this document.

The culmination of the benefits (savings, capital treatment, financial incentives) should then be compared against the total cost of ownership (third party plus internal resource costs) of SBOM solutions.

## Example Business Case

The following section is an example of how a business leader might organize thoughts on a business case. This is not meant to be an exhaustive list or a suggested approach, but rather as a springboard of ideas that should be tailored for the specific use cases and circumstances that apply.

For this case, we will consider a U.S. Power Utility that generates \$10 billion in annual revenue with roughly 10,000 employees.

These savings of roughly \$4Mn presented in the table below should be compared against the spend in vulnerability management; application security; and governance, risk, and compliance (GRC) which are collectively estimated at \$12.0Mn (or \$7.2Mn when excluding GRC)<sup>31</sup>. Savings, therefore, are at a magnitude of 33% to 55% of the annual spend on relevant IT security initiatives.

By extrapolating the \$4Mn savings potential to over 1,000 major global companies of comparable size (excluding the impact on small and medium-sized businesses) and extending this analysis over a 10-year period, the data indicates an unseen \$40 billion challenge in the software supply chain.

---

<sup>31</sup> The Gartner *IT Key Metrics Data 2023: IT Security Measures — Analysis* shows that the utilities sector spends \$1.20 in IT security per thousand dollars of revenue, and 41% is allocated to vulnerability management and security analytics, 19% to application security, and 24% to governance, risk, and compliance. Thus, \$10Bn revenue x 1.20/1,000 x (41% + 19% + 24%) = \$12.0 Mn in relevant IT security spend (or \$7.2 Mn when excluding the 24% for GRC).

*Notes for smaller organizations:*

- *Some rows may be entirely irrelevant.*
- *While smaller organizations will have smaller savings, they will also have smaller required investments.*
- *Other rows should consider higher costs for per-unit labor costs (due to, for example, a small entity relying on managed security service providers instead of internal labor).*
- *Small organizations may experience higher loss probabilities (potentially due to a less mature control environment).*
- *Greater volatility may be considered (e.g., higher software switching costs due to more frequent changes).*
- *Wide variances may exist between actual versus benchmarked metrics (e.g., software as percentage of revenue may be irrelevant to entities with homogeneous revenue streams).*

Use Case & Benefit	Baseline, Annual (\$)	Est. Savings (%)	Estimated Savings, Annual (\$)	Discussion
<b>IT/OT Security Use Cases</b>				
<b>Vulnerability Incident Response</b>  <i>Faster incident response time</i>	<b>\$200,000</b> <i>Cost of incident response investigation</i>	<b>80%</b>	<b>\$160,000</b>	<p><b>Baseline:</b> Estimated annual vulnerability incident response triage and investigation costs. 5 cybersecurity FTE x \$150,000 salary x 1.33 loading factor<sup>32</sup> x 10 weeks of investigation per year / 50 working weeks = \$200,000. The baseline could be much larger if leveraging high-cost contractors.</p> <p><b>Savings:</b> Log4j, for example, would result in hours instead of weeks of research due to manual methods such as (i) scanning assets as plugins become available, (ii) log analysis, (iii) network monitoring, (iv) remote log in and inspection, (v) onsite inspections, (vi) penetration testing, and (vii) reviewing intelligence feeds. 1 week of research (40 hours) is reduced to 8 hours leading to 80% savings.</p>
<b>Third-Party Risk Mgmt.</b>  <i>Improved efficacy of TPRM program</i>	<b>\$200,000</b> <i>Additional resource to review vendor SSDLC</i>	<b>75%</b>	<b>\$150,000</b>	<p><b>Baseline:</b> As the importance of ensuring vendors have a secure software development lifecycle (SSDLC) process, so does the cost to a vendor risk management program. Incremental costs to perform validated evaluations of critical vendor SSDLC and semi-automated evaluation of non-critical vendor SSDLCs may range from 0.50 to 2 FTE depending on the depth of review and existing systems in place. Assume 1.0 subject matter expert at \$150,000 x 1.33 loading factor.</p> <p><b>Savings:</b> Purpose-built SBOM risk management systems that are fully integrated with the vendor risk management process will eliminate 75% to 100% of the incremental effort depending on the level of service offered by the solution.</p>
<b>Architecture Review</b>  <i>Architecture Review Efficiencies</i>	<b>\$200,000</b> <i>Additional resource to review software supply chain</i>	<b>100%</b>	<b>\$200,000</b>	<p><b>Baseline:</b> A cybersecurity architecture team may need to be expanded to evaluate the software supply chain risks. A team of three or four may seek to add another resource at a cost of \$150,000 x 1.33 loading factor.</p> <p><b>Savings:</b> By having an SBOM management system that is fully integrated with the architecture review process, the existing team will see minimal incremental work.</p>
<b>Threat Hunting</b>  <i>Efficiencies for automated processes</i>	<b>\$600,000</b> <i>Additional resources to monitor anomalous components</i>	<b>67%</b>	<b>\$400,000</b>	<p><b>Baseline:</b> Additional monitoring techniques should be employed to ensure that critical systems have not suffered from a supply chain attack. One method for checking integrity using SBOMs includes comparing the SBOMs from deployed software (typically via agents from an endpoint detection &amp; response system) to the expected SBOMs received from a supplier or those tested in a secure sandbox environment using installers that have been pre-verified for integrity and authenticity. Without a purpose-built system in place, this could increase manual efforts required by 2 to 4 FTE. Assume 3 cybersecurity personnel at \$200,000 loaded.</p> <p><b>Savings:</b> With an automated reconciliation process, additional FTE may not be required as the existing team may be able to manage. On a conservative basis, assume only 1 FTE is required or a 67% reduction from 3.</p>
<b>Vulnerability Management</b>	<b>\$245,000</b> <i>Annual exposure</i>	<b>80%</b>	<b>\$195,000</b>	<p><b>Baseline:</b> Using stats from IBM's breach report, the estimated annual cost of a data breach in the U.S. is \$9.44 and that 13% of breaches are due to vulnerabilities<sup>33</sup>. As a second reference point, the Information Risk Insights Study (IRIS) by Cyentia Institute</p>

<sup>32</sup> Loading factor of 1.33 accounts for the additional direct costs per employee but does not consider management overhead. Loading factor could be as much as 1.48 when factoring all items such as bonus (10%); medical insurance (10%); employer-paid taxes for Medicare, Social Security, local unemployment & disability insurance (8%); other benefits such as retirement matching, reimbursed training or health incentives (5%); IT and facilities costs (10%); and overhead allocations for shared services such as HR, finance, legal, compliance, security (5%).

<sup>33</sup> IBM. 2022 *Cost of a Data Breach Report*, p. 7-17. <https://www.ibm.com/downloads/cas/3R8N1DZJ>



Use Case & Benefit	Baseline, Annual (\$)	Est. Savings (%)	Estimated Savings, Annual (\$)	Discussion
<i>Efficiencies in expanded scope of vuln. mgmt. programs to component</i>	<i>from incidents resulting from software vulnerabilities</i>			<p>shows that 22% of companies with \$10Bn-\$100Bn in revenue have at least one cyber event with a 0.91x factor for utilities<sup>34</sup>. Assuming the event impacted 3 million records (roughly the customer base of a \$10Bn utility company), the loss magnitudes in the IRIS report (with some math and assumptions) corroborate the IBM report loss magnitude at higher amounts<sup>35</sup>.  \$9.44Mn loss x 13% due to vulnerabilities x 22% probability x 0.91 probability adjustment for utilities = \$245k</p> <p><b>Savings:</b> Assumes that defenders armed with SBOM component-level vulnerability management can reduce the loss probability by 80% due to additional diligence and insight. These savings exclude the efficiency gains related to labor cost savings.</p>
<b>Procurement Use Cases</b>				
<b>Pre-Purchase Security Review</b>  <i>Avoid Software Purchases with Material Technical Debt</i>	<b>\$2,500,000</b>  <i>Switching costs for material software per year</i>	<b>6%</b>	<b>\$156,000</b>	<p><b>Baseline:</b> An estimated 1.25% of revenue for U.S. power utilities is spent on software<sup>36</sup> x \$10bn revenue assumed; this is \$125Mn/year in software costs. Switching costs are estimated between 5% and 20% depending on software complexity; assume 10% for switching costs. Thus, switching costs will be \$12.5Mn. Software may be replaced every 5 years on average or \$2.5Mn switching cost per year.</p> <p><b>Savings:</b> Assumes that (i) software with significant findings (significant volume of components at end-of-life support, unsupported dependencies, copyleft requirements) is not likely to keep up with changing market demands, (ii) that it will have a 50% higher likelihood of needing to be replaced at the end of the term, (iii) average term is 5 years, (iv) that 25% of acquired software has material issues, and (v) leveraging an SBOM solution, 50% of these purchases will be avoided.</p> <p>\$2.5Mn/year switch costs x 50% replacement rate x 25% affected software x 50% switching cost avoided = \$156k.</p>
<b>Contract Conditions</b>  <i>Contract Negotiations for Better Software</i>	<b>\$2,500,000</b>  <i>Switching costs for material software per year</i>	<b>17%</b>	<b>\$420,000</b>	<p><b>Baseline:</b> Assume the same \$2.5Mn switching costs per year defined in the Pre-Purchase Security Review above.</p> <p><b>Savings:</b> Assumes average software life is extended only one year from 5 years to 6 years, thus \$12.5Mn switching costs / 6 years is \$2.08Mn/year, which is a savings of \$420k/year (when compared to switching every 5 years).</p>
<b>Compliance Use Case</b>				
<b>Licensing Compliance</b>	<b>\$100,000</b> <i>Additional resource to review</i>	<b>100%</b>	<b>\$100,000</b>	<p><b>Baseline:</b> While there have been many legal cases and losses due to licensing non-compliance, the frequency is not sufficient to use a loss estimate as the baseline for a software consumer use case. Instead, companies may choose to view the cost in terms of staffing a licensing compliance function for which the incremental cost to incorporate software supply chain security may be 0.50 FTE for a subject matter</p>

<sup>34</sup> Cyentia. 2022 IRIS Report, p. 9-10. [https://www.cyentia.com/wp-content/uploads/IRIS-2022\\_Cyentia.pdf](https://www.cyentia.com/wp-content/uploads/IRIS-2022_Cyentia.pdf)

<sup>35</sup> Page 17 of the Cyentia 2022 IRIS report shows that when 1Mn records are affected by a cyber event, the loss probabilities are \$10Mn x 23.8% + \$100Mn x 5.7% + \$1Bn x 0.7% which sums to \$15Mn which is directionally close (given the liberties taken in record count assumptions) to IBM's 2022 Cost of Data Breach Report which cites \$9.44Mn as the average cost of a cyber event in the US.

<sup>36</sup> Gartner Forecast: Enterprise IT Spending for the Power and Utilities Market, Worldwide, 2020-2026 report shows that 26% of IT spend (2023 estimated) is on software. IT Key Metrics Data 2023: Industry Measures — Insights for Midsize Enterprises indicates 4.9% is spent on IT. This is 1.27% (26% x 4.9%) of revenue.

Use Case & Benefit	Baseline, Annual (\$)	Est. Savings (%)	Estimated Savings, Annual (\$)	Discussion
<i>Efficiencies in Compliance Staffing</i>	<i>component licensing</i>			expert or 1 FTE of a less senior resource. Assume a 1 FTE baseline of \$75,000 x 1.33 loading factor or \$100,000.  <b>Savings:</b> With an SBOM risk analysis solution and system that can connect to the existing tools used by the licensing (or procurement, legal, or compliance – depending on who owns licensing risk) team – the additional effort will be minimal and additional FTE may not be required.
<b>Vulnerability Mandates</b>  <i>Efficiencies in Compliance Staffing</i>	<b>\$500,000</b> <i>Additional resources to investigate SBOM vulnerabilities</i>	<b>60%</b>	<b>\$300,000</b>	<b>Baseline:</b> Assume a 10-person team will need to expand another 5 FTE at \$75,000/ea with 1.33 loading factor to investigate SBOM vulnerabilities.  <b>Savings:</b> Using a cybersecurity risk management system that includes SBOM and integrates with existing vulnerability management tooling, resource expansion could be limited substantially. Assume only 2 of 5 FTE are required (3 FTE savings).
<b>Attestation and SBOM Collection</b>  <i>Efficiencies in Compliance Staffing</i>	<b>\$100,000</b> <i>Additional resource to manage in legacy manner</i>	<b>100%</b>	<b>\$100,000</b>	<b>Baseline:</b> When companies have a compliance requirement and no system, the default is often SharePoint and Excel – both great tools but lack the out-of-the-box compliance automation desired for these use cases (vendor document collection, audit logging, reminders, dashboards, alerts, role-based access control, etc.). Baseline assumes that additional resources should be added. Assume 1 full time risk management personnel at \$75,000 x 1.33 loading factor or \$100,000.  <b>Savings:</b> Comprehensive SBOM risk management solutions may have automation capabilities and managed services for vendor outreach; thus, the incremental internal effort may be avoided entirely.
<b>Operational Use Cases</b>				
<b>Investing</b>  <i>Negotiation Leverage in M&amp;A Activities</i>	<b>\$30,000,000</b> <i>Average annual M&amp;A involving software</i>	<b>2.0%</b>	<b>\$600,000</b>	<b>Baseline:</b> This scenario may vary widely by entity. Assume that mergers and acquisitions average 1.5% of revenue over the long term or \$150Mn on this \$10Bn annual revenue scenario. Assume that 20% of acquisition dollars relate to companies providing software (e.g., innovative distributed energy resource companies with software, improving operational efficiency, improving customer service, other innovations). \$150Mn x 20% = \$30Mn.  <b>Savings:</b> Improved visibility will assist in negotiation with a wide range of likely outcomes depending on the type of risks uncovered and even the savings from avoiding a bad deal altogether. Assume a conservative 2% savings from avoiding losses due to technical debt or from increased negotiation leverage.
<b>Operational and Mission Readiness</b>  <i>Avoid Lengthy Consulting Projects to Achieve Risk Awareness</i>	<b>\$900,000</b> <i>Consulting &amp; custom dashboard creation &amp; maintenance</i>	<b>80%</b>	<b>\$180,000</b>	<b>Baseline:</b> Companies seeking to provide dashboard rollups of combined vendor and product (hardware & software) risks often have to stitch multiple systems together and utilize expensive consulting firm rates. A rollup dashboard with change management support (but excluding the internal change management cost) from a large consulting firm with a well-defined scope could consume 2,000 to 4,000 labor hours with bill rates averaging \$300-\$500/hour. Assume 3,000 hours at \$300/hr.  <b>Savings:</b> A supply chain cybersecurity platform with SBOM capabilities could deliver significant implementation savings with pre-built connectors and purpose-built for describing mission & operational readiness. Assume 60% savings amortized over three years or 20% annualized. Savings may continue beyond the three-year period due to lower maintenance and update costs.

Use Case & Benefit	Baseline, Annual (\$)	Est. Savings (%)	Estimated Savings, Annual (\$)	Discussion
<b>Efficient Internal Code Development</b>  <i>Higher Software Quality</i>	<b>\$9,000,000</b>  <i>Internal software development for large utility</i>	<b>10%</b>	<b>\$900,000</b>	<p><b>Baseline:</b> 30 engineers x \$150,000 salary x 1.33 loading factor x 1.5 for support roles (development operations, product management, design, database, testing, release mgmt.)</p> <p><b>Savings:</b> 10% of baseline driven by (i) reduced unplanned, unscheduled work, (ii) reduced code bloat, (iii) adequate planning for dependencies within complex projects, (iv) prevention of rework due to licensing complexities, (v) monitor components for vulnerabilities, (vi) avoidance of use of components nearing end-of-life support, and (vii) easier code reviews.</p>
<b>Grand Total</b>			<b>\$3,861,000</b>	

## How to Apply Business Cases

The business cases with savings should be applied only in the context of the applicable environment. Here are some practical considerations when tailoring this to another environment.

1. Determine which use cases will be deployed in the short term versus long-term. Faster payback periods get faster buy-in.
2. Adjust scenarios to the relevant environment (investment sizing, already-planned initiatives, risk reduction objectives).
3. Add up the savings by use case and compare with the SBOM investment. Return on investment will be calculated as  

$$([business\ case\ savings] - [ongoing\ cost\ of\ SBOM\ solution]) / [initial\ cost\ of\ SBOM\ solution]$$



## APPENDIX 7: SBOM RESOURCES



## NTIA SBOM Resources

The National Telecommunications and Information Administration's (NTIA) multistakeholder process drove the SBOM initiative from 2018 until it was handed over to CISA in 2021<sup>37</sup>. NTIA's collection of works is published and often referenced and has been incorporated into the new CISA working groups (2021-2023).

Documents are grouped in topical areas.<sup>38</sup>

- **Introduction to SBOM:** *SBOM at a Glance (2021), SBOM FAQ (2021), SBOM Myths vs. Facts (2021), SBOM Explainer Videos on YouTube (2020-2021)*
- **Understanding SBOM:** *Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) (2021), SBOM Options and Decision Points (2021), Use Cases: Roles and Benefits for SBOM Across the Supply Chain (2019), SBOM Tool Classification Taxonomy (2021)*
- **SBOM Implementation:** *Survey of Existing SBOM Formats and Standards (2021), Software Suppliers Playbook: SBOM Production and Provision (2021), Software Consumer Playbook: SBOM Acquisition, Management, and Use (2021), How-To Guide for SBOM Generation (2021), Sharing and Exchanging SBOMs (2021)*
- **Technical Resources:** *Software Identity: Challenges and Guidance (2021), SBOM Tool Classification Taxonomy (2021), Vulnerability-Exploitability eXchange (VEX) – An Overview (2021)*
- **Lessons from the Proof-of-Concept Work:** *How-To Guide for SBOM Generation in Healthcare (2021), Healthcare SBOM Proof of Concept – Phase II Summary (2021), Healthcare Proof of Concept Report (2019)*
- **Other Resource:** *Software Bill of Materials Related Efforts (2021), Software Identity: Challenges and Guidance (2021), SBOM Two-Page Overview (2020); NTIA Minimum Elements of an SBOM (2021)*

## CISA Working Groups

CISA took over the NTIA efforts regarding SBOM in 2021 and holds several working groups to drive adoption of software transparency initiatives.

*CISA will advance the SBOM work by facilitating community engagement, development, and progress, with a focus on scaling and operationalization, as well as tools, new technologies, and new use cases. This website will also be a nexus for the broader set of SBOM resources across the digital ecosystem and around the world.*

---

<sup>37</sup> CISA. Software Bill of Materials (SBOM). <https://www.cisa.gov/sbom>

<sup>38</sup> NTIA. Software Bill of Materials. <https://ntia.gov/page/software-bill-materials>

*An SBOM-related concept is the Vulnerability Exploitability eXchange (VEX). A VEX document is an attestation, a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities – CISA SBOM website.<sup>39</sup>*

Featured documents and updated meeting times may be obtained from the CISA SBOM website:

<https://www.cisa.gov/sbom>

To join the working groups, send an email request to [SBOM@cisa.dhs.gov](mailto:SBOM@cisa.dhs.gov) stating the groups of interest.

### **SBOM Working Groups**

- Vulnerability Exploitability eXchange – Mondays at 10a ET
- Sharing & Exchanging – Mondays at 12p ET
- On-Ramps & Adoption – Tuesdays at 12p ET
- Cloud & Online Applications – Wednesdays at 3p ET
- Tooling & Implementation – Thursdays at 3p ET

### **Events**

- SBOM-a-Rama 2022 (Dec 15, 2022) – Various topics; slides are available.  
<https://www.cisa.gov/resources-tools/resources/cisa-sbom-rama>
- SBOM-a-Rama 2023 (Jun 14, 2023) – Various topics; slides are available.  
<https://www.cisa.gov/news-events/events/sbom-rama>

### **CISA SBOM Documents**

- Secure Software Development Self-Attestation Common Form – Apr 27, 2023  
<https://www.cisa.gov/resources-tools/resources/secure-software-self-attestation-common-form>
- Minimum Requirements for Vulnerability Exploitability eXchange – Apr 21, 2023<sup>40</sup>  
<https://www.cisa.gov/resources-tools/resources/minimum-requirements-vulnerability-exploitability-exchange-vex>
- SBOM Sharing Lifecycle Report – Apr 17, 2023<sup>41</sup>  
<https://www.cisa.gov/resources-tools/resources/software-bill-materials-sbom-sharing-lifecycle-report>
- Types of Software Bill of Material (SBOM) – Apr 21, 2023<sup>42</sup>  
<https://www.cisa.gov/resources-tools/resources/types-software-bill-materials-sbom>

---

<sup>39</sup> CISA. Software Bill of Materials (SBOM). <https://www.cisa.gov/sbom>

<sup>40</sup> CISA. “CISA Releases Two SBOM Documents”. <https://www.cisa.gov/news-events/alerts/2023/04/21/cisa-releases-two-sbom-documents>

<sup>41</sup> CISA. “CISA and CESER Releases Software Bill of Materials (SBOM) Sharing Lifecycle Report”. <https://www.cisa.gov/news-events/alerts/2023/04/17/cisa-and-ceser-releases-software-bill-materials-sbom-sharing-lifecycle-report>

<sup>42</sup> CISA. “CISA Releases Two SBOM Documents”. <https://www.cisa.gov/news-events/alerts/2023/04/21/cisa-releases-two-sbom-documents>



- VEX Use Case Document – Apr 1, 2022  
<https://www.cisa.gov/resources-tools/resources/vulnerability-exploitability-exchange-vex-use-case-document-april-2022>
- VEX Status Justification – Jun 1, 2022  
<https://www.cisa.gov/resources-tools/resources/vulnerability-exploitability-exchange-vex-status-justification-document-june-2022>

## **Anticipated NATF Operationalizing SBOM**

A joint initiative between NATF, DOE, DHS, INL, Fortres Information Security, and others is underway to provide further guidance on practical SBOM implementations. This is expected to be released in 2023.



Fortress guides critical enterprises to discover, prioritize, and  
monitor cyber and operational supply chain risk.  
Find out more at [www.fortressinfosec.com](http://www.fortressinfosec.com).

