

# Enhancing Cybersecurity Best Practices with Software Bill of Materials (SBOM)

August 2, 2021

An overview of SBOMs and related cybersecurity  
frameworks for critical infrastructure

---

Tobias Whitney  
VP Industry Relations and Regulatory Affairs

Tony Turner  
VP Security Solutions

Bryan Cowan  
Supply Chain Research Analyst

# Table of Contents

## White Paper

01. Background	3
02. Framework: SBOMs and NERC CIP Compliance	5
SBOMs & NERC CIP Compliance	5
Do NERC CIP Standards Require Software to be Secure?	5
NERC CIP-013-1 Supply Chain Risk Management	5
SBOM analysis as a foundation for an effective cyber risk management plan	6
CIP-007-6 R2	6
CIP-010-3 R1.6	7
CIP-010-3 R3.1 and 3.2	7
03. Implementation: Establishing the Utility as a Supplier	9
NIST Cybersecurity Framework (CSF)	10
NIST SP 800-53	10
NIST SP 800-161	11
NIST SP 800-171 & Cybersecurity Maturity Model Certification (CMMC)	11
IEC 62443	12
National Defense Authorization Act (NDAA)	13
EEI Model Procurement Language	13
ISO 27001	13
DOE C2M2	14
NATF Supplier Criteria	15
04. Appendix	16
05. References	25

# 01. Background Framework & Implementation

## 01

Electric power organizations must purchase, deploy and manage software associated with critical infrastructure to ensure effective and reliable operations. It is challenging enough to plan, design and construct the most complicated interconnected machine on earth—today's grid is controlled by and highly dependent on sophisticated software.

In less than six months, we have seen cybersecurity incidents at Solar Winds, Colonial Pipeline, and Kaseya that have all been a direct result of ineffective software security controls. With the increased complexity of software, it has become increasingly important that cybersecurity practices focus on the elimination of malicious code into control system software. Modern software

can contain hundreds of software components and can consist of pieces of third-party code (either proprietary or open source) that have been incorporated into the product by the supplier. This paper examines a solution to this challenge through the lens of Software Bill of Materials (SBOMs). As described by the National Telecommunication and Information Administration:

An SBOM provides those who produce, purchase, and operate software with information that enhances their understanding of the supply chain, which enables multiple benefits, most notably the potential to track known and newly emerged vulnerabilities and risks.

# An effectively prepared and analyzed SBOM can be invaluable in addressing critical infrastructure cybersecurity challenges.

## How do we ensure security and transparency in our software supply chain?

The US Government has recognized the potential value of SBOMs via an Executive Order (EO) issued on May 12, 2021. It requires the National Institute of Standards and Technology (NIST) to issue guidance to enhance the security of the software supply chain by February 6, 2022 (US President 2021, 26638). This includes supplier guidance on providing the federal government an SBOM for each purchased product.

If a utility were to engage their vendors regarding SBOMs, which CIP Standards or other regulatory frameworks, would support the use of SBOMs? What standards frameworks or requirements would dictate whether software is secure and that the evidence of security is transparent to the user and supplier? This white paper will exam-

ine various regulatory frameworks electric power organizations may navigate in pursuit of software security and how of SBOMs can be used as an effective vehicle to mitigate third-party software risks.

Ultimately, the benefit of SBOMs is to provide actionable information to purchasers so that they may make informed decisions about software and help to 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.

## 02. Framework

# SBOMs and NERC CIP Compliance

## 02

### SBOMs & NERC CIP Compliance

The NERC Critical Infrastructure Protection Standards (CIP) do not specify “how” entities comply; however, they do tend to specify “what” control objectives are needed to mitigate a risk to the Bulk Power System. Therefore, there are numerous means and methods a utility could use to comply with a given requirement, that are not explicitly stated in the standards language itself; that is much of the case for SBOMs. The more appropriate question to ask regarding NERC CIP compliance is: “How can SBOMs help me comply with the NERC CIP standards and improve my security posture as a utility?” This is the question that is examined more closely in this section.

### Do NERC CIP Standards Require Software to be Secure?

In short, the NERC CIP Standards do specify the security of Bulk Electric System (BES) Cyber Systems. Part of a BES Cyber System is software, so indirectly, the CIP Standards do require the security of software assets (or the systems associated with those assets) that may have real-time impact to the reliable operations of the grid. If software requires security, then SBOMs can be used to help achieve security. Not only are software assets need-

ed to be secured, but several CIP standards mandate that those software assets are secured in certain ways. The following CIP Standards can be used to help ensure that grid software is protected:

- CIP-013-1
- CIP-007-6 R2
- CIP-010-3 R1.6
- CIP-010-3 R3.1 and 3.2

Let’s examine the requirements and use case for SBOMs in each requirement throughout the following sections.

### NERC CIP-013-1 Supply Chain Risk Management

The first requirement reads:

*“R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems (software). The plan(s) shall include...*

*1.1 One or more process(es) used in planning...to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from...procuring and installing vendor equipment and software...<sup>1</sup>”*

---

<sup>1</sup> Note that some phrases from R1.1 that were not necessary for addressing the requirement.

SBOM should be provided by the software supplier or solution provider as a means to **evaluate the security and inherent risk of an application** prior to implementation.



SBOM analysis is an important foundation for an effective cyber risk management plan.

As previously noted, BES Cyber Systems contain software, and an effective risk management plan must account for risks that stem from procuring and installing this software. The first step in mitigating risk starts with acknowledging or enumerating the risks in list format. There is a myriad of issues regarding a list, but for the sake of this paper, we will assume that the list requirement in CIP-002 is acceptable by the industry.

SBOMs do an excellent job at listing the components of software. In fact, one could argue how an entity could even mitigate the risk of software without knowing what the software consists of. Once the SBOM of key grid components is known, an entity could be much more systematic and transparent in mitigating those risks. To be clear, CIP-013 does not mandate a SBOM is required for compliance to CIP-013-1 R1.1, however,

it stands to reason that including SBOM requirements in a utility Supply Chain Risk Management Plan would support an effective implementation of this requirement. For instance, a compliant Supply Chain Risk Management Plan could include language that requires that an SBOM is provided by the software supplier or solution provider as a means to evaluate the security and the inherent risk of the application prior to its implementation on the grid.

#### CIP-007-6 R2

CIP-007-6 R2 is the requirement for patch management. It requires a regular cycle of steps (repeated every 35 days), each of which has its own Requirement Part. The first step is described in R2.2: "At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1."

To understand how SBOMs could be applied in this use case, patch management,

one must review the language of this standard more closely – especially this phrase: “evaluate security patches for applicability.” Entities are supposed to be able to discern security-related patches from non-security related patches. If an entity had a detailed list of software components from the vendor of their product, as well as information regarding which component the patch is applicable to, an entity could then make a more informed decision as to whether the patch could impact the security of the device in question.

Currently, today’s practice is reliant on the supplier’s release notes to make the determination of applicability and security impact to the systems in question. A validated SBOM (an SBOM that has been independently assessed by a third party) would be an effective means to comply with CIP-007-6 R2, as well as an effective security practice that would provide the entity with a greater ability to make decisions about patching and mitigating software-borne vulnerabilities. In addition, having information about third-party software or open-source components within a BCS application would be helpful to entities so that they can determine other mechanisms of use to help mitigate those risks. There is an obvious compliance and security improvement capability here that could be unlocked with SBOMs.

### CIP-010-3 R1.6

CIP-010-3 R1.6 was added to R1 when CIP-013-1 came into effect. It addresses the following two risks:

1. Ensuring the software or patch when accessed by the entity, can be trusted and authenticated to the supplier through non-repudiation.
2. Ensuring that the software or patch is free of malicious code before it is introduced to critical infrastructure.

While the most widely used methods to verify software identity and integrity includes examining the digital signature and hash value, these may not always be available. Even if they are available, the entity may prefer to get a “second opinion” from independent sources.<sup>2</sup> In either of these cases, the user (or a third party acting on their behalf) could request a validated SBOM, digital signature and hash value. They could then compare this to a recent SBOM for the same product to determine if they are similar. If the two are significantly different, this could indicate a compromise or detected malware within the BCS in question. This type of analysis, that SBOMs can enable, could identify critical red flags and warn the user to avoid installing the downloaded software.

### CIP-010-3 R3.1 and 3.2

CIP-010-3 3.1 and 3.2 are requirements that mandate that vulnerability assessments are performed to assess the security of BES Cyber Systems. R3.1 requires that an active or paper-based vulnerability assessment is performed every 15 calendar months. R3.2 is similar but requires that high impact BES

---

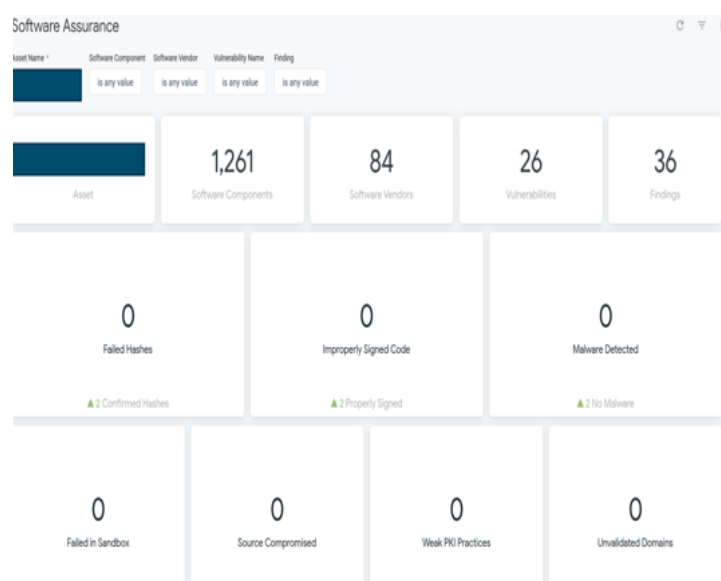
<sup>2</sup> <https://fortressinfosec.com/solutions/file-integrity-assurance>

It is critical to **enumerate, analyze and identify** vulnerabilities that reside at the software component level to mitigate software-borne, zero-day exploits that could adversely impact the reliable operations of critical infrastructure.

Cyber Systems are assessed via an active vulnerability assessment. In either case, the control being applied is needed to identify vulnerabilities on key systems. This requirement is not exclusive for software. In fact, the requirements do not specify how the vulnerability assessment (paper or active) is performed. If the utility has concerns about the vulnerability of the software and applications used to manage their grid assets, an SBOM could be a key tool to help enumerate, analyze and identify if vulnerabilities reside at the software component level. This could help reduce the risk of software-borne, zero-day exploits that could significantly impact the reliable operations of the grid.

Figure 1. Summary Output of SBOM Analysis

Shown below is a summary output SBOM analysis performed by Fortress Information Security. Vulnerabilities are identified at the software component level, along with a series of other relevant information that can help the CIP Senior Manager determine if the BES Cyber Systems have software-level vulnerabilities.



Additional information that could be derived from a SBOM-based vulnerability assessment:

- Number of (Software) Components
- List of Fourth-Party Vendors supplying software components
- Vulnerabilities– based on public vulnerability sources
- Failed Hash Analysis
- Code Signing Analysis
- Malware Detection Analysis
- Source Identification Analysis
- PKI Practices

## 03. Implementation

# Establishing the Utility as a Supplier

### 03

Many utilities are beginning to recognize the need to address supplier concerns not only as a purchaser, but also as a supplier to other entities, critical infrastructure or critical defense facilities (CDI). When supporting CDI with energy management services, microgrids or distributed energy resources, requirements are dictated by the federal facility that the utility is servicing. In this case, the NERC CIP standards may not have jurisdiction, but a different contingent of standards and regulations may be applicable.

The Biden Administration's Executive Order 14028 could change the software security landscape for organizations servicing CDI.

On June 26, 2021, NIST released a definition of "critical software," defining the scope of this class of software as any software that has, or has direct software dependencies upon, one or more components with at least one of the following attributes (National Institute of Standards and Technology 2021b, 3):

- Designed to run with elevated privilege or manage privileges
- Has direct or privileged access to networking or computing resources
- Is designed to control access to data or operational technology
- Performs a function critical to trust

- Operates outside of normal trust boundaries with privileged access

Using this definition, the NIST has come up with a preliminary listing of the categories of software it considers to be covered by this definition; this includes software for Identity, Credential, and Access Management (ICAM), operating systems, hypervisors, web browsers, endpoint security, network monitoring and configuration, network protections, remote scanning, and remote access, and backup and recovery software (National Institute of Standards and Technology 2021b, 4-8).

When the final guidelines are published in 2022, it is expected SBOMs will be required for products eligible for federal procurement. A minimum viable SBOMs standard with extensions for other industries, along with federal agency use of these standards will push adoption of SBOMs to federal suppliers and their subcontractors. As NIST guidelines are commonly used across many U.S. industries the EO will have the effect of promoting SBOMs adoption broadly.

In addition to the EO, the following standards frameworks have applications for SBOMs:

- NIST Cyber Security Framework
- NIST SP 800-53
- NIST SP 800-161
- NIST SP 800-171 & Cybersecurity Maturity

- ty Model Certification (CMMC)
- IEC 62443
- National Defense Authorization Act (NDAA)
- EEI Procurement Language
- ISO 27001
- Department of Energy C2M2
- NATF Criteria and Questionnaire

### NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) was developed to improve cybersecurity risk management in critical infrastructure, for example, electric power utilities and their Industrial Control Systems (ICS) (National Institute of Standards and Technology 2018). The heart of the CSF is the Framework Core. This consists of a set of Functions, which are made up of Categories; the Categories are made up of Subcategories. The Subcategories are worded as high-level mitigations that can be applied to mitigate cybersecurity risks. The risk(s) mitigated by each subcategory are not stated in the Core, but they can be inferred from the wording of the Subcategory.

For example, the first Subcategory is ID.AM-1: “Physical devices and systems within the organization are inventoried.” One of the risks behind ID.AM-1 could be stated as: “A physical system might be surreptitiously introduced onto an organization’s network. However, due to not having an up-to-date inventory of devices on the network, the organization might not learn that the system is there. The system might then be used to launch a cyberattack on other systems on the network.” Six Subcategories are tied to risks that might be mitigated if the organization has access to

SBOMs. Table 1 in the Appendix shows a listing of those Subcategories, as well as a short description of how SBOMs could help in mitigating the risks behind those controls.

### NIST SP 800-53

The National Institute of Standards and Technology (NIST) special publication 800-53, “Security and Privacy Controls for Information Systems and Organizations,” is a catalog of security and privacy controls to protect organizational operations and assets from a diverse set of threats and risks. These controls are designed with a risk management approach in mind, and classify controls based on the impact a component may have on the confidentiality, integrity and availability of the system, for example, high, moderate, and low (National Institute of Standards and Technology 2020, 1-3).

Relevant controls related to SBOMs can be found in section CM-8, “System Component Inventory.” This control asks an organization to develop and document an inventory of system components that is discrete, identifies information technology assets and includes hardware, software and firmware. It recommends updating the inventory as system components are installed, updated or removed (National Institute of Standards and Technology 2020, 107-108). Section CM-2 also recommends documenting a baseline configuration of an information system, and the use of automated tools to track version numbers and patches of operating systems, application and current patch levels (National Institute of Standards and Technology 2020, 97-98). Table 1 in the Appendix shows a listing of the relevant controls and how SBOMs can help.

A minimum viable SBOM standard with extensions for other industries, coupled with federal agency use of these standards will **encourage adoption of SBOMs** among federal suppliers and their subcontractors.

#### NIST SP 800-161

NIST SP 800-161 covers, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” and gives guidance to federal agencies on supply chain risks in their information and communications technology (ICT) systems that may contain potentially malicious functionality, are counterfeit or are vulnerable due to poor manufacturing and development practices (National Institute of Standards and Technology 2015).

For “high impact systems,” NIST SP 800-161 requires agencies to develop organizational Supply Chain Risk Management (SCRM) requirements for suppliers to include in contracts. It also requires them to develop procedures to detect counterfeit and compromised ICT products before deployment in an operational environment (NASA 2021). Analysis of SBOM data can be used to understand if counterfeit or vulnerable components are present before deployment into an operational environment.

The framework’s set of security controls for (SCRM) are organized into “Families.” The controls are mitigations for risks that can be inferred from their wording. As in the case of the NIST CSF (discussed above), the risks that are “behind” those controls can

be mitigated if SBOMs are available. Table 1 in the Appendix shows a listing of the relevant controls and how SBOMs can help.

#### NIST SP 800-171 & Cybersecurity Maturity Model Certification (CMMC)

The National Institute of Standards and Technology (NIST) special publication 800-171 covers protecting Controlled Unclassified Information (CUI) in the federal government. This framework provides security requirements for protecting the confidentiality of CUI when the information is processed, stored or transmitted in nonfederal systems and organizations. The US government depends on many contractors for products and services who need to handle federal data to provide these services. This unclassified information can affect the operations of federal agencies, so protection of the data while on nonfederal systems is important to continue normal operations (National Institute of Standards and Technology 2021a, 1). Table 1 in the Appendix shows a listing of the relevant controls and how SBOMs can help.

The Cybersecurity Maturity Model Certification (CMMC) is an evolution of other federal cybersecurity standards, including NIST SP 800-171. Its requirements include assessments of organizations’ cybersecurity prac-



tices and processing, in addition to assessments of technical systems (Evans 2021). It requires contractors to have a current NIST SP 800-171 assessment. CMMC is a major change for government contractors and the Department of Defense (DoD) will phase in stricter standards over the next few years on assessing contractor compliance of cybersecurity requirements (Marx 2021).

CMMC standards were developed by the DoD to protect defense contractors from cyberattacks. The DoD will require an organization to be certified as compliant with CMMC standards before awarding any contracts. An Accreditation Body (AB) will certify third-party inspectors who will certify organizations against the different CMMC levels. The standards started rolling out January 31, 2020, and by 2026 all-new DoD contracts will require suppliers to be CMMC certified (Evans 2021).

### IEC 62443

International Electrotechnical Commission (IEC) 62443 series of standards was developed to address the issue of security for industrial automation and control systems (IACS) in the industrial process sector, but IACS are also found in other industries, such as power and energy supply and distribution, and transport. These standards are more appropriate for IACS than other standards more suited to information and communications technology, as they have different performance and availability requirements, as well as equipment lifetime (IEC Editorial Team 2021). Cyber-attacks on IACS can threaten critical infrastructure and potentially have environmental or public health consequences as well.

The standards take a risk-based approach to cybersecurity, based on the concept that

it is not possible to try to protect all assets in equal measure. Instead, organizations must identify what is most valuable and requires the greatest protection and identify vulnerabilities (IEC Editorial Team 2021). These standards have some relevance to SBOMs. IEC 62443 Part 4-1 of the standards requires, as part of vulnerability testing, software suppliers should deliver a composition analysis on all binary executable files. Table 1 in the Appendix shows a listing of the relevant controls and how SBOMs can help.

### National Defense Authorization Act (NDAA)

Many utilities also support Critical Defense Facilities (CDF), or military facilities, and as such are already subject to such regulations as the 2019 National Defense Authorization Act, Section 889. This rule prohibits certain suppliers such as Huawei, Hikvision, Dahua, and other adversarial manufacturers from supplying hardware components to the Federal government, as well as utilities providing power to the CDF (US Congress, 2018, 283). As the Federal Acquisition Regulation (FAR) is being evaluated for change based on Executive Order 14028 proscribing the use of SBOM and other software supply chain requirements, utilities should track the federal procurement rules closely to understand any downstream impacts for their procurement and supply chain risk management programs (US President 2021, 26634).

The 2021 National Defense Authorization Act (NDAA), enacted by Congress, includes new cybersecurity provisions to improve the cybersecurity posture of the US. This includes tasking the Defense Department with developing a plan for the annual as-

# Utilities should track federal procurement rules closely to understand downstream impacts to their supply chain risk management programs.

assessment of cyber vulnerabilities of major weapon systems (US Congress 2020, 700). Numerous provisions will impose new requirements, including expectations of government contractors. Several of these requirements would be aided using SBOMs. Table 1 in the Appendix shows a listing of the relevant sections and how SBOMs can help.

## EEI Model Procurement Language

The Edison Electric Institute developed model contract language to address cyber supply chain risk and encourage adoption by the vendor community. This language is focused on processes required by the NERC supply chain risk management reliability standard, CIP-013-1 Requirement 1, Part 1.2. The model is a starting point for negotiations with vendors and service providers, and not a specific framework for utility companies (Edison Electric Institute 2021). The model language designed to provide utilities a consistent set of provisions to address CIP-013-1 security controls within their own respective contractual forms. Table 1 in the Appendix shows a listing of the relevant requirements and how SBOMs might apply.

## ISO 27001

The International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC), created this international standard focused on information security. The standards are generalized and applicable to organizations in many industries and can be scaled to the needs of the business. The standard focuses on the establishment and implementation of an Information Security Management System (ISMS) (ISO 2013, 6-7). ISO 27001 specifies the requirements to implement, monitor, maintain and continually improve the ISMS to bring information security under management control. The standard also includes best practices for documentation requirements, divisions of responsibility, availability, access control, security, auditing and corrective and preventive measures (Vidich 2021). Table 1 in the Appendix shows a listing of the relevant ISO 27001 controls and how SBOMs might apply.

## DOE C2M2

The Department of Energy (DOE) has included Third-Party Risk Management (Section 6.7) and Cyber Security Architecture (Section 6.9) in Cyber Capability Maturity

Model version 2.0.<sup>3</sup> While there are no regulatory mandates that requirement the implementation of C2M2 or to achieve a certain maturity level, the guidance and practices included are invaluable and do provide ample references to controls that can be further supported or enhanced by SBOMs. The Third-Party Risk Management section proposes to address the following:

Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties, commensurate with the risk to critical infrastructure and organizational objectives

C2M2 has identified for MIL3 (the highest maturity level for a given category) that cybersecurity requirements include secure software and secure product development practices in third-party risk management programs. The C2M2 also includes criteria consideration for organizations to consider end-of-life or end-of-support in their third-party programs. SBOMs data can support both control objectives.

Within C2M2 Cybersecurity Architecture section, software security is stressed throughout this section of cybersecurity capabilities, which states the following:

Establish and maintain the structure and behavior of the organization's cybersecurity architecture, including controls, processes, technologies and other elements,

commensurate with the risk to critical infrastructure and organizational objectives.

One of the architecture domains includes a dedicated subsection on software security which includes controls consideration for the following topics<sup>4</sup>:

- In-house software development
- Procured software and third-party development practices
- (Software) architecture review process for new and revised applications
- Authenticity checks for all software
- Security testing (static testing, dynamic testing, fuzz testing, pen testing) for software

### NATF Supplier Criteria

The North American Transmission Forum (NATF) has coordinated with the industry to develop a set of standard practices to help the effective and consistent interactions between grid purchasers and suppliers. Their dedicated webpage for the Supply Chain Security Initiative states the following:

The NATF and other industry organizations are working together to provide a streamlined, effective, and efficient industry-accepted approach for entities to assess supplier cyber security practices. The model, if applied widely, will reduce the burden on suppliers so their efforts with purchasers can be prioritized and entities can be pro-

---

<sup>3</sup> <https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>

<sup>4</sup> [https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021\\_508.pdf](https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf)

vided with more information effectively and efficiently. The industry organizations collaboration effort is focused on improving cyber security, and assisting registered entities with compliance to regulatory requirements.

The NATF Supply Security Criteria has a cybersecurity control section dedicated to addressing Application Software Security which addresses many controls that SBOMs can enable. Here are several examples that NATF has listed:

- Supplier has a documented program for secure product development, including applying security controls and secure coding techniques, within the system development life cycle
- Supplier establishes and maintains a security management program that validates the authenticity and origins of third-party hardware, firmware and software including open-source code software
- Supplier establishes and maintains a security program for the product or service being purchased, including implemented processes to verify the integrity and authenticity of the software, patches and firmware relevant to the product or service being delivered to the entity
- Supplier uses secure central software repository after software, patches and firmware authenticity and integrity have been validated, so that authenticity and integrity checks do not need to be performed before each installation
- Supplier digitally signs and validates software, patches and firmware prior to distribution
- Provide any countries other than the United States or Canada in which supplier's product (i.e. hardware, software, firmware or components) is manufactured or developed (indicate if none)

---

<sup>5</sup> <https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>

## 04. Appendix

Table 4.1 Summary of Cybersecurity Framework Controls Relationships to SBOMs

Control	Control Description	SBOM Solution
<b>NERC Critical Infrastructure Protection Standards<sup>6</sup></b>		
<b>CIP-013-1 R1.1</b>	“One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software”	An SBOM is essential to a full understanding of cyber supply chain risks for a product. This can include a lack of patching and support, and non-announced component end-of-life status. Aids in evaluating vendors’ products and their commitment to secure development.
<b>CIP-007-6 R2.2</b>	“At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.”	SBOMs will provide more transparency and clarity for entities to identify and apply relevant security patches to critical applications or systems.
<b>CIP-010-3 R1.6</b>	“1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.”	An SBOM is essential to a full understanding of cyber supply chain risks for a product. This can include a lack of patching and support, and non-announced component end-of-life status. Aids in evaluating vendors’ products and their commitment to secure development.
<b>CIP-010-3 R3.1 and 3.2</b>	“At least once every 15 calendar months, conduct a paper or active vulnerability assessment... perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment;”	The average software product has 135 components. A vulnerability management plan which doesn’t take account of vulnerabilities due to components of a software product, in addition to the supplier’s code, will inevitably omit a majority of the vulnerabilities found in that product.

<sup>6</sup> <https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>

Control	Control Description	SBOM Solution
<b>NIST Cybersecurity Framework (CSF) <sup>7</sup></b>		
<b>ID.RA-1</b> <b>p. 26</b>	"Asset vulnerabilities are identified and documented"	Having SBOMs for the asset or the software installed on it will permit identification of more vulnerabilities. These vulnerabilities will be unknown without an SBOM.
<b>ID.RA-5</b> <b>p. 27</b>	"Threats, vulnerabilities, likelihoods, and impacts are used to determine risk"	Having SBOMs for the asset and/or the software installed on it will permit identification of more vulnerabilities. A true risk assessment for an asset requires SBOMs.
<b>ID.SC-2</b> <b>p. 28</b>	"Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process"	Suppliers of components of a software product cannot be known by customers of that product unless the customer has an SBOM.
<b>PR.IP-12</b> <b>p. 36</b>	"A vulnerability management plan is developed and implemented"	The average software product has 135 components. A vulnerability management plan which doesn't take account of vulnerabilities due to components of a software product, in addition to the supplier's code, will inevitably omit a majority of the vulnerabilities found in that product.
<b>DE.CM-8</b> <b>p. 39</b>	"Vulnerability scans are performed"	If the software owner has an SBOM, they will know about vulnerabilities in at least some components, as well as vulnerabilities in the supplier's own code. Then they will be able to scan for both types of vulnerabilities.
<b>RS.MI-3</b> <b>p. 43</b>	"Newly identified vulnerabilities are mitigated or documented as accepted risks"	The software owner doesn't have a complete list of vulnerabilities in any software product unless they know about vulnerabilities in the components of that product. This requires an SBOM.

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

Control	Control Description	SBOM Solution
<b>NIST SP 800-53<sup>8</sup></b>		
CM-8 (a) p. 108	"Develop and document an inventory of system components"	SBOMs would support a higher level of granularity in a component inventory not previously possible.
CM-8 (b) p. 108	"Review and update the system component inventory"	SBOMs allow for easier implementation of automated tools for version monitoring and keeping the inventory up- to-date.
CM-2 (a) p. 97	"Develop, document, and maintain under configuration control, a current baseline configuration of the system"	SBOMs could aid in documenting the baseline configuration and detect the presence of unauthorized software or firmware components and serve as a central database of components to quickly find systems affected by newly discovered vulnerabilities.
CM-2 (2) p. 97	"Automation support for Accuracy and Currency"	SBOM formats could be machine read and processed to periodically update system components baseline.
<b>NIST SP 800-161<sup>9</sup></b>		
CM-10 (1) p. 78	"Software Usage Restrictions -Open-Source Software"	Open-source components included in a software product can lead to licensing risk. They can also lead to supply chain security risks, such as lack of patching and support, and non-announced component end-of-life status. Having an SBOM is essential to fully understanding licensing and supply chain cyber risks for software.

<sup>8</sup> <https://doi.org/10.6028/NIST.SP.800-53r5><sup>9</sup> <https://doi.org/10.6028/NIST.SP.800-161r1-draft>

Control	Control Description	SBOM Solution
PV-2 p. 95	"Tracking Provenance and Developing a Baseline"	While it is not always possible, it is important to try to learn the provenance of every component of software used by your organization. That will usually be a supplier name (in the case of proprietary components) or a URL or download location (in the case of open-source components). This information should be available in the SBOM, for every component. Not having this available for one or more components, raises serious questions about a software supplier that includes components of unknown provenance.
SI-1 p. 115	"System and Information Integrity Policy and Procedures"	The compromise of the SolarWinds Orion build process provided a vivid example of loss of integrity in the software supply chain. Because of the great sophistication of the attackers, that attack couldn't have been prevented with an SBOM; however, less sophisticated attacks of the same type could often be detected by a supplier who generates SBOMs regularly during the build process, especially if component hash values are included.
SI-2 p. 115	"Flaw Remediation"	Most software suppliers are diligent in patching security vulnerabilities in code they wrote themselves. However, many are less diligent in patching vulnerabilities in third-party components in their software. Unless their customers have an SBOM, they can't identify component vulnerabilities at all, let alone track the supplier's response to them. If they have an SBOM and VEX documents, they can identify component vulnerabilities and, if the supplier is slow about patching them, following up with a timetable.

Control	Control Description	SBOM Solution
SI-7 p. 116	"Software, firmware, and Information Integrity"	Just as it's important for energy industry organizations to verify both integrity and authenticity of any software or patch they download, it's also important for a software supplier to do the same for components it downloads, whether from proprietary suppliers or open-source repositories. While there is no way for a software customer to check a digital signature for a component of a product they own, just releasing an SBOM may prompt suppliers to be more diligent about verifying authenticity and integrity of components.
<b>NIST SP 800-171<sup>10</sup></b>		
3.4.1 p. 20	"Establish and maintain baseline configurations and inventories of organizational systems"	SBOMs would support a higher level of granularity in a component inventory not previously possible and allow for a centralized system of component inventories.
3.11.1 p. 33	"Periodically assess the risk to organizational operations and assets"	The availability of SBOMs for the asset and/or the software installed on it will permit identification of many more vulnerabilities than otherwise.
3.11.2 p. 33-34	"Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities identified"	With an SBOM, a federal contractor will be able to scan for vulnerabilities in components, as well as vulnerabilities in the supplier's own code.
3.11.2 p. 34	"Remediate vulnerabilities in accordance with risk assessments"	With SBOM and VEX documents, they can identify component vulnerabilities and prioritize remediation based on the severity of the flaw.

<sup>10</sup> <https://doi.org/10.6028/NIST.SP.800-171r2>

Control	Control Description	SBOM Solution
<b>IEC 62443<sup>11</sup></b>		
IEC 62443 4-1 5.11 SM-9 p. 24	"Identify and manage the security risks of all externally provided components used within the product"	An SBOM is essential to a full understanding of cyber supply chain risks for a product. This can include a lack of patching and support, and non-announced component end-of-life status. Aids in evaluating vendors' products and their commitment to secure development.
IEC 62443 4-1 9.4 SVV-3 p. 36	"Software composition analysis on all binary executable files, including embedded firmware, delivered by the supplier"	Having SBOMs for the software, or the software installed on it, will permit identification of many more vulnerabilities than otherwise. These vulnerabilities will be unknown without an SBOM. Machine-readable file formats also allow for easier linking to the National Vulnerability Database to understand the severity of a flaw.
<b>National Defense Authorization Act (NDAA)<sup>12</sup></b>		
NDAA 2019 Section 889 p. 282-283	"Prohibition on Certain Telecommunications and Video surveillance surveys or equipment"	While it is not always possible, it is important to try to learn the provenance of every component of software used by your organization. That will usually be a supplier name (in the case of proprietary components) or a URL or download location (in the case of open-source components). This information should be available in the SBOM, for every component, allowing a DoD contractor to prevent themselves from using components from unapproved foreign countries
NDAA 2021 Section 1712 p. 700-701	"Develop a plan for the annual assessment of cyber vulnerabilities of major weapon systems"	Having SBOMs available for the software installed on major weapon systems would enable the DoD to understand which components are up-to-date, determine whether they are at potential risk of a newly discovered vulnerability, and respond quickly to new vulnerabilities.

<sup>11</sup> <https://webstore.iec.ch/publication/33615>

<sup>12</sup> <https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf>  
<https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf>

Control	Control Description	SBOM Solution
<b>EEI Model Procurement Language<sup>13</sup></b>		
Hardware, Firmware, Software, and Patch Integrity and Authenticity Proposed Language (e) p. 11	"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."	An SBOM is essential to a full understanding of cyber supply chain risks for a product. Risks include a lack of patching and support, and non-announced component end-of-life status. Aids in evaluating vendor's products and their commitment to secure development.
Hardware, Firmware, Software, and Patch Integrity and Authenticity	"Contractor shall identify or provide Company with a method to identify the country (or countries) of origin of the procured Contractor product and its components (including hardware, software, and firmware). Contractor will identify the countries where the development, manufacturing, maintenance, and service for the Contractor product are provided. Contractor will notify Company of changes in the list of countries where product maintenance or other services are provided in support of the procured Contractor product. This notification in writing shall occur at least 180 days prior to initiating a change in the list of countries.	This information should be available in the SBOM, for every component. Not having this available for one or more components, raises questions about a supplier that includes components of unknown provenance.
Proposed Language (d) p. 10-11		The provenance should include a supplier name (in the case of proprietary components) or a URL or download location (in the case of open-source components).
<b>ISO 27001:2013<sup>14</sup></b>		
Control A.8.1.1 p. 17	"Inventory of assets"	SBOMs would support a higher level of granularity in a component inventory not previously possible.

<sup>13</sup> <https://www.eei.org/issuesandpolicy/Documents/EEI%20Law%20-%20Model%20Procurement%20Contract%20Language.pdf>

<sup>14</sup> <https://www.iso.org/isoiec-27001-information-security.html>

Control	Control Description	SBOM Solution
Control A.12.6.1 p. 22	"Management of technical vulnerabilities"	The availability of SBOMs for software components of the information system permits the identification of many more vulnerabilities. These vulnerabilities will be unknown without an SBOM. A software owner doesn't have a complete list of vulnerabilities in any software product unless they know about vulnerabilities in the components of that product.
Control A.15.1.3 p. 25	"Information and communication technology supply chain"	SBOM requirements in agreements with suppliers provides a more complete understanding of cyber supply chain risks for a product. This information allows for easier evaluations of vendor's products and their commitment to secure development

#### Department of Energy Cybersecurity Capability Maturity Model (C2M2)<sup>15</sup>

6.7 Third Party Risk Management 2. Manage Third-Party Risks p. 43	"i. Selection criteria include consideration of end-of-life and end-of-support timelines j. Selection criteria include consideration of safeguards against counterfeit or compromised software, hardware, and services	
6.9 CyberSecurity Architecture 4. Implement Software Security as an Element of Cybersecurity Architecture p. 53	f. The architecture review process evaluates the security of new and revised applications prior to deployment g. The authenticity of all software and firmware is validated prior to deployment h. Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing)	SBOMs can support software architecture reviews by providing evidence of software components. Validation of software sources can be enabled by SBOMs. Security testing of software can be designed to address software components which can improve the security profile of application in question.

<sup>15</sup> [https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021\\_508.pdf](https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf)

Control	Control Description	SBOM Solution
North American Transmission Forum (NATF) Supplier Criteria <sup>16</sup>		
Criteria 48: Vulnerability Management	Supplier establishes and maintains a security management program that validates the authenticity and origins of third-party hardware, firmware and software including open source code software	SBOMs can support the validation of the authenticity and origins of third-party firmware and software. Open source software would be more easily identified via SBOMs.
Criteria 49: Vulnerability Management	Supplier establishes and maintains a security program for the product or service being purchased, including implemented processes to verify the integrity and authenticity of the software, patches and firmware relevant to the product or service being delivered to the entity	

<sup>16</sup> <https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>

## 05. References

International Electrotechnical Commission. 2018. "Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements." IEC International Standard 62443-4-1, ed. 1.

IEC Editorial Team. 2021. "Understanding IEC 62443." IEC News & Blogs." February 26. Accessed July 2, 2021.  
<https://www.iec.ch/blog/understanding-iec-62443>

Edison Electric Institute. 2020. Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk, Version 2.0. Edison Electric Institute, May. Accessed July 28, 2021.  
<https://www.eei.org/issuesandpolicy/Documents/EEI%20Law%20-%20Model%20Procurement%20Contract%20Language.pdf>

Edison Electric Institute. 2021. "Cyber & Physical Security." EEI.org. Accessed July 28, 2021.  
<https://www.eei.org/issuesandpolicy/Pages/Security.aspx>

Evans, Corbin. 2021. "NDIA Resources on CMMC". National Defense Industrial Association. Accessed July 3, 2021.  
<https://www.ndia.org/policy/cmmc>

Department of Energy; Office of Cybersecurity, Energy Security, and Emergency Response. "Cybersecurity Capability Maturity Model (C2M2)". July 2021. Accessed July 28, 2021.  
<https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>

ISO. 2013. IISO/IEC 27001 – Information technology — Security techniques — Information security management systems — Requirements, 2nd ed. ISO/IEC, October 1. Accessed July 28, 2021.  
<https://www.iso.org/isoiec-27001-information-security.html>

Marx, Tyson. 2021. "The DOD's New CMMC Requirements and the False Claims Act". Ward & Berry Blog, May 10. Accessed July 3, 2021.  
<https://www.wardberry.com/the-dods-new-cmmc-requirements-and-the-false-claims-act/>

NASA. 2021. Standards Crosswalk ISO 20243 & NIST 800-161, NASA Solutions for Enterprise-Wide Procurement. April 12. Accessed June 23, 2021.  
[https://www.sewp.nasa.gov/documents/OTTPS-NIST\\_CrossWalk\\_NASA\\_SEWP.pdf](https://www.sewp.nasa.gov/documents/OTTPS-NIST_CrossWalk_NASA_SEWP.pdf) .

North American Electric Reliability Corporation. 2015. CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments. March. Accessed July 2, 2021.

<https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-3.pdf>

North American Electric Reliability Corporation. 2016. CIP-002-5.1a — Cyber Security — BES Cyber System Categorization. December 14. Accessed July 2, 2021.

<https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf>

North American Electric Reliability Corporation. 2018. CIP-013-1 – Cyber Security - Supply Chain Risk Management. October 18. Accessed July 2, 2021.

<https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf>

North American Transmission Forum (“NATF”) Supply Chain Security Criteria. June 4, 2021. Accessed July 2, 2021.

<https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>

Sonatype, Gene Kim, and Dr. Stephen Magill. 2020. 2020 State of the Software Supply Chain. Accessed July 17, 2021.

<https://www.sonatype.com/resources/white-paper-state-of-the-software-supply-chain-2020>

Rivero, Nicolas. “What is a supply chain cyber attack?”. Quartz, July 6. Accessed July 14, 2021.

<https://qz.com/2030053/what-is-a-supply-chain-cyber-attack/>

US Cyberspace Solarium Commission. 2020. Cyberspace Solarium Commission Final Report. March. Accessed July 14, 2021.

[https://drive.google.com/file/d/1ryMCIL\\_dZ30QyjFqFkkf10MxIXJGT4yv/view](https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view)

US Department of Commerce, National Institute of Standards and Technology. 2015. NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations, by John Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol. April 1. Accessed June 25, 2021.

<https://csrc.nist.gov/publications/detail/sp/800-161/final>

US Department of Commerce, National Institute of Standards and Technology. 2018. Framework for Improving Critical Infrastructure Cybersecurity. April 16. Accessed June July 17, 2021.

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

US Department of Commerce, National Institute of Standards and Technology. 2020. NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations, by Joint Task Force. September. Accessed July 4, 2021.

<https://doi.org/10.6028/NIST.SP.800-53r5>

US Department of Commerce, National Institute of Standards and Technology. 2021a. NIST Special Publication 800-171 Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations by Ross, Ron, Victoria Pillitteri, Kelley Dempsey, Mark Riddle, Gary Guissanie. January 28. Accessed July 17, 2021.

<https://doi.org/10.6028/NIST.SP.800-171r2>

US Department of Commerce, National Institute of Standards and Technology. 2021b Definition of Critical Software Under Executive Order (EO) 14028. June 25. Accessed June July 1, 2021.

[https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL\\_1.pdf](https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf)

# Enhancing Cybersecurity Best Practices with a Software Bill of Materials (SBOM)

**[www.fortressinfosec.com](http://www.fortressinfosec.com)**

Fortress Information Security, LLC  
1.855.FORTRESS  
189 S. Orange Avenue  
Orlando, FL 32801

© Fortress Information Security, LLC. All rights reserved. All other brands, products, or service names are or may be trademark or service marks of their respective owners. This document, prepared by Fortress Information Security, contains confidential work product for the exclusive use of its clients. Duplication, distribution or use for anything other than its intended purpose is prohibited.