INL/RPT-22-68847
Revision 0

Towards Software Bill of Materials in the Nuclear Industry

September 2022

A primer on the current SBOM ecosystem and a recommended "crawl, walk, run" approach for seamlessly integrating an SBOM program in nuclear power plants

Shannon Eggers, Tori Simon, Baleigh Morgan, Ethan Bauer
Idaho National Laboratory

Drew Christensen
Pacific Northwest National Laboratory

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Batelle Energy Alliance, LLC

INL/RPT-22-68847
Revision 0

Towards Software Bill of Materials in the Nuclear Industry

A primer on the current SBOM ecosystem and a recommended "crawl, walk, run" approach for seamlessly integrating an SBOM program in nuclear power plants

Shannon Eggers, Tori Simon, Baleigh Morgan, Ethan Bauer
Idaho National Laboratory

Drew Christensen
Pacific Northwest National Laboratory

September 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Cybersecurity Crosscutting Technology Development Program
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

ABSTRACT

Large, modern industrial facilities often incorporate thousands of digital assets in their operational technology. Regulated facilities, such as nuclear power plants (NPPs), maintain robust cybersecurity and configuration management programs that often use bills of materials (BOMs) for these assets, including make, model, and version of hardware, firmware, and software. However, these BOMs typically capture only first- or second-tier information provided by the original equipment manufacturer (OEM). Unfortunately, as indicated by the increasing number and sophistication of software supply chain attacks, this level of detail is insufficient for identifying all the potential vulnerabilities and risks in software applications. Software BOMs (SBOMs) provide detailed enumeration of components and dependencies within the product or devices, including firmware. SBOMs can be combined with vulnerability data sources and vendor vulnerability attestations to improve vulnerability management and enable rapid identification of affected components when new software vulnerabilities are discovered. Ideally, SBOMs are created by the OEM prior to installation. However, since this practice is not yet commonplace and since NPPs are typically slow to adopt new technology, most NPPs do not incorporate SBOMs into their asset or configuration management programs. Fortunately, SBOMs can be generated by NPPs on existing digital assets to provide further insight into risk management decisions. This report provides an overview of the current SBOM ecosystem and recommends guidance on how to get started in a "crawl, walk, run" manner to develop and implement a sustainable SBOM program for digital assets in an NPP.

Page intentionally left blank

ACKNOWLEDGEMENTS

We would like to thank each of our Reviewers who spent their valuable time reviewing and providing insightful feedback to improve this report.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

BOM	bill of materials
CDA	critical digital asset
CESER	Office of Cybersecurity, Energy Security & Emergency Response
CISA	Cybersecurity and Infrastructure Security Agency
CPE	common platform enumeration
CSAF	Common Security Advisory Framework
C-SCRM	cyber supply chain risk management
CVE	common vulnerabilities and exposures
DBT	design basis threat
DHS	Department of Homeland Security
DOE	Department of Energy
EO	Executive Order
IAEA	International Atomic Energy Agency
ICT	information and communications technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NVD	National Vulnerability Database
NPP	nuclear power plant
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
O&M	operating and maintenance
OEM	original equipment manufacturer
OSS	open-source software
OT	operational technology
PM	preventive maintenance
PURL	package URL
SBOM	software bill of materials
SCAP	Security Content Automation Protocol
SPDX	Software Package Data Exchange
SRI	security-related information
SWHID	software heritage identification
SWID	software identification
URL	uniform resource locator
UUID	universal unique identifier
VEX	Vulnerability Exploitability eXchange

Page intentionally left blank

Towards Software Bill of Materials in the Nuclear Industry

1. INTRODUCTION

The concept of a bill of materials (BOM) for the manufacturing industry has existed since the early 1900's [1]. Similarly, the concept of a software bill of materials (SBOM) has existed, at least in some form, since the onset of modular software development. As the use of open-source software and third-party tools and libraries has expanded, so has the awareness that better tracking and transparency of software components is needed, especially for security purposes. For example, consider the Apache Log4j vulnerability disclosed in December 2021—the vulnerability in this logging library used in many proprietary and open-source Java-based applications, including operational technology (OT), allows adversaries to achieve remote code execution and take full control of a system [2]. SBOMs enable quick answers to questions, such as "am I affected?" and "where am I affected?," as new supply chain incidents arise [3]. Thus, when the Log4j vulnerability was disclosed, an asset owner lacking full visibility into their complete inventory of software components likely required a long time to determine if, and in which systems, Log4j was present. On the other hand, a facility that had implemented an SBOM program could quickly search and find all instances of Log4j in their operational environment.

In the past several years, industry groups have been actively developing new SBOM standards and processes. The National Telecommunications and Information Administration (NTIA) launched a Multistakeholder Process on Software Component Transparency in 2018 to formulate and establish common consensus definitions, proof of concept case studies, and educational materials. In May 2021, Executive Order (EO) 14028, Improving the Nation's Cybersecurity, was issued, directing NTIA to develop minimum elements for an SBOM. EO 14028 also directed the National Institute of Standards and Technology (NIST) to issue guidance to enhance the security of the software supply chain, including criteria for establishing integrity, provenance, and SBOM by software developers. Both the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security & Emergency Response (CESER) have also set up working groups to further explore and promote the adoption of SBOMs.

The threat landscape is constantly changing—new vulnerabilities are continuously discovered and adversaries continuously advance their tactics, techniques, and procedures. Not only do SBOMs help increase transparency in supply chains, which can directly improve software development practices and reduce vulnerabilities, but SBOMs provide transparency at nuclear power plants (NPPs). This transparency can directly reduce cyber risk by improving other plant programs, such as configuration management, vulnerability management, and software quality assurance. This report first provides a brief background on the current SBOM ecosystem, including vendor vulnerability attestations and industry activities, before describing a "crawl, walk, run" approach to seamlessly implementing an SBOM program at an NPP. This report also provides guidance on how to adapt the process new reactor builds.

2. BACKGROUND

2.1 Software Bill of Materials

2.1.1 What is an SBOM?

Traditionally, a bill of materials (BOM) is a comprehensive list, including quantity, of raw materials, components, subcomponents, subassemblies, and assemblies required to build or manufacture a product. Similarly, an SBOM is a complete listing of all open-source and proprietary software components and subcomponents (e.g., source code, executables, libraries, and modules) and their dependencies. Since SBOMs are expected to include firmware, they are essentially an inventory of all "ingredients" in a digital asset, with the exception physical hardware components (e.g., integrated circuits, assemblies). Hardware BOMs are not covered in this report.

Using terminology from NTIA, EO 14028 defines an SBOM as a "formal record containing the details and supply chain relationships of various components used in building software [4]." It further highlights the usefulness of SBOMs for each stakeholder in the supply chain, noting that software end users should use SBOMs to reduce cyber risk by easily determining if their organization is susceptible to discovered vulnerabilities.

In the U.S., many NPPs maintain records, such as equipment databases and configuration control data sheets, that identify the make, model, and versions of primary hardware and software for installed digital assets. While these data sheets are useful, they typically only include high-level data without drilling down into all the unique software components that comprise the digital asset.

The main utility of SBOMs is not as standalone data; their primary usefulness occurs through integration with other tools and data sources. For instance, an SBOM cannot provide a risk analysis score for a digital asset, and it cannot be used by itself to evaluate supply chain risk. However, when comprehensive SBOMs are used in conjunction with vulnerability data and vulnerability management programs, they can enable cross-reference of software components to known vulnerabilities which can then be used for risk prioritization and risk treatment decisions. Further use cases are identified in Section 2.1.3.

The number of components and dependencies in software can be extensive and is often best structured as a graph database rather than a tree, or hierarchical, database. Existing NPPs have thousands of digital assets installed in their facilities. Additionally, procurement of new digital assets will likely include extensive SBOM data from many different suppliers. Thus, to facilitate the sheer volume of software components and the related data for all digital assets at an NPP, some level of automation for both creation and ongoing monitoring of the SBOM ecosystem is preferred. To allow for functionality, efficiency, and flexibility in these semi-automated systems, standardized, machine-readable, structured data formats are required.

2.1.2 Baseline SBOM Elements

In 2018, the NTIA started a multistakeholder process on software transparency. As a result of EO 14028, this working group developed a baseline set of elements to uniquely and unambiguously identify SBOM components and their relationships [5]. Table 1 identifies baseline data fields that should be tracked and maintained for each component and subcomponent. Table 2 identifies baseline requirements that are needed to enable automation or semi-automation in the SBOM ecosystem. And finally, Table 3 lists preferred baseline practices for SBOM programs.

Table 1. Baseline data fields for an SBOM (adapted from [3] and [5]).

Data Field	Description
Author Name	The author or entity who created the SBOM. The author may not always be the supplier. [SBOM-level metadata]
Timestamp	Data and time when the SBOM was created or last updated. A common international format should be used. [SBOM-level metadata]
Component Name	Designation or identifier assigned to component. The component name is defined by the original supplier. This data field should include the capability to handle multiple names or aliases.
Component Version	Version of the identified component. This identifier is used by the supplier to specify software changes. If a component does not have a version, the author should create one.
Supplier Name	Name or other identifier of the supplier for a component. This data field should include the capability to handle multiple names or aliases. The supplier may not always be the author.
Component Hash*	Cryptographic hash that is an intrinsic identifier for the software component. This field is recommended, but not required. It may be beneficial to provide multiple hashes for a component or collection of components (e.g., hash for source, hash for compiled binary, and hash for the collection). Digital signatures can used but they add additional complexity with requirements for key management and signature verification. The hash generation method should be made available so it can be reproduced.
Unique Identifier(s)	Additional information to uniquely identify a component. This may be generated relative to a global unique hierarchy or namespace or reference an existing global coordinate system. Examples include Common Platform Enumeration (CPE), Package URL (PURL), Universal Unique Identifier (UUID) (also known as Globally Unique Identifier [GUID]), and Software Heritage ID (SWHID). The component hash may also effectively function as a unique identifier.
Relationship	Association between SBOM components. The default relationship type is *includes*, which represents the inclusion of or dependency on a separate upstream component. The inverse, *included in*, may also be used. Either direction can be used as long as one direction is chosen and used consistently. It is a *primary* relationship if the component has no upstream dependencies; a primary component defines the subject of the SBOM.
License Information*	Identifies license(s) and license term(s).

* Recommended but not required.

Table 2. Baseline requirements to enable automation or semi-automation in the SBOM ecosystem (adapted from [5]).

Requirement	Description
Automatic Generation	Capability to automatically generate an SBOM. This may also include automatic integration with other tools, such as vulnerability management.
Machine-Readability	Formatting of SBOM data fields into common, machine-readable formats for use by the international ecosystem.
Data Formats	Standardized data formats to generate and consume SBOMs. Standard formats include Software Package Data Exchange (SPDX), CycloneDX, and Software Identification (SWID) tags. These formats are further described in Section 2.1.5.

Table 3. Preferred baseline practices in an SBOM program (adapted from [5]).

Practices	Description
Frequency	A new SBOM should be created whenever a software component is updated with a new build or release and whenever new details or an error in the SBOM is discovered.
Depth	At minimum, an SBOM should contain all primary, or top level, components with all transitive dependencies listed. Going deeper into the graph will provide greater transparency. The depth can be specified by the consumer by indicating the number of transitive steps required in an SBOM or by specifying depth in operational terms (e.g., all non-open-source software, all components of a certain function).
Known Unknowns	The author must explicitly identify cases in which the full dependency graph is not enumerated (e.g., known unknowns). This provides clear distinction between components with no further dependencies and components for which the presence of dependencies is unknown and incomplete. This is implemented in the Relationship data field.
Completeness*	All data field values should be completed. If no related SBOM value, the entry should explicitly define values that differentiate between no assertion (data is missing) and no value (not applicable).
Distribution and Delivery	SBOMs and SBOM revisions should be made available (and ingestible) in a timely fashion to those who need them. This includes how the existence and availability is made known and how the SBOM is retrieved or transmitted to those who have the appropriate permissions to access them.
Access Control	SBOMs may be made public or may be kept confidential, depending on the organization creating them. If access control is desired, these terms must be specified through licensing, contracts, or other mechanisms regarding software use and rights.
Accommodation of Mistakes	As SBOM programs are implemented, a process for handling omissions or errors is required. While striving for perfection is optimum for software assurance and supply chain risk management, it is better to start the SBOM process and provide corrections as needed as the process evolves. Consumers should be explicitly tolerant of occasional incidental errors (but not tolerant of intentional obfuscation or willful ignorance).

* Not specifically listed by [5].

There are often challenges with supplier and component namespaces, especially with legacy digital assets that are installed in the NPP. Mergers, acquisitions, and ownership transfers may result in supplier name changes as well as product line/model name changes. Consider the following examples:

1. A digital asset was installed in an NPP ten years ago. The supplier or OEM of the asset has changed ownership three times. Each time ownership changed, the component name was changed.
2. A software vendor decides to rebrand their company. In doing so, they change their product line names, which effectively changes the component name.
3. An OEM added a digital component to a product but maintained the same model name.

Note that these situations may also occur at a subcomponent level, adding further complexity.

When researching the data fields for a component to include in an SBOM for legacy assets, it may not be straightforward to identify the current supplier or component names. Theoretically, according to the practices listed in Table 3, supplier and component name changes should result in an SBOM revision and a link from the old SBOM to its successor should be created to maintain revision history. While this is the ideal case when purchasing new assets, it is often untenable for legacy assets as this history is often unknown and it may be challenging to map an older supplier/component name to the current supplier/component name. Additionally, the supplier may no longer exist.

The unique identifier can be constructed using persistent uniform resource locator (PURL) syntax for each component. The NTIA provides the following syntax for creating this identifier [6]:

scheme:type/namespace/name@version?qualifiers#subpath

where:

scheme: (pkg)
type: (supplier)
namespace: **Supplier Name**
name: **Component Name**
version: **Version String**
qualifiers#subpath (optional, not used)
pkg:supplier/<Supplier Name>/<Component Name>@<Version String>

2.1.3 The benefits of SBOMs

The full benefits of SBOMs are recognized when integrated with other data and tools. The transparency provided by SBOMs allows for extended capabilities in component analysis, such as enhancing integrity, assurance, and security as outlined in Table 4. A primary benefit using tools to link SBOMs with vulnerability data and vendor vulnerability attestations is the ability to continuously monitor the environment to determine vulnerability status of components and dependencies. This feature provides exceptional situational awareness and reduces the time to identify and remediate newly discovered vulnerabilities. This enhanced transparency into installed software components greatly improves an NPP's security posture.

Of course, it is important to note what an SBOM is not—it is not by itself a risk management or vulnerability management tool. SBOMs cannot identify malware on systems and they cannot identify when software was built with compromised developer tools, such as compilers or math engines. The largest benefits occur when tools are integrated together within the larger SBOM ecosystem.

Table 4. SBOM-integrated use cases and benefits (adapted from [7]).

SBOM Use Cases	Description and Benefits
Asset Inventory and Configuration Management	Maintaining an SBOM and linking it with a facility's Configuration Management program enables better capabilities for maintaining design basis as well as improving maintenance and troubleshooting activities. SBOMs provide a rapid method for answering "where used" queries and can aid in the license management process.
Vulnerability Management	Using an SBOM with vulnerability data sources and a vulnerability management system can provide an expanded level of insight into potential vulnerabilities. Section 2.2 provides additional details on the use of SBOMs with vulnerability data and vendor vulnerability attestations.
Pedigree	An SBOM can provide detailed information on the software pedigree. Pedigree describes the lineage, or origins, of how the components have come together and the process under which they came together, including compiler details and settings [8]. Pedigree captures the history of how the component was produced or derived, which can provide information on whether software is hardened against specific attacks or vulnerabilities.
Provenance	An SBOM can provide detailed information on software provenance. Provenance describes the chain of custody, or traceability, of all authorship, build, release, packaging, and distribution across the entire supply chain [8]. Provenance plays an important role in determining Foreign Ownership, Control, or Influence (FOCI). This can aid in identification of prohibited software and avoidance of software from banned countries. It also provides organizations with supplier information for assistance with product updates and bug tracking.
Integrity & Authenticity	Verifying component hashes and unique identifiers for the components and collection of components included in SBOMs can provide a cryptographic basis that the asset has not been altered or substituted without authorization.
Assurance	Using SBOMs in coordination with other processes, such as vulnerability data sources, vulnerability management systems, assessments, design reviews, attack surface analysis, and verification and validation, can improve capabilities to assure software is secure, safe, and resilient.
Cyber Risk Management	Cyber risk analysis is the process of determining the vulnerabilities, threats, and consequences of intentional or unintentional adverse events on a digital asset. SBOMs enumerate the software components, enabling additional insight into cyber risk to improve risk prioritization and risk treatment. Enhanced cyber hygiene directly improves cybersecurity, leading to improved insurance ratings and premiums.
Cyber Supply Chain Risk Management (C-SCRM)	SBOMs do not replace C-SCRM activities. They work with other data sources to improve supply chain risk analysis capabilities. When SBOM data and vulnerability data is linked or mapped with supply chain data (e.g., supply chain lifecycle, provenance, pedigree, and supplier trustworthiness data), the extensibility provided by this confluence of data will lead to greater risk insights within your supply chain, thereby resulting in better supply chain risk management decisions.

2.1.4 An SBOM Myth: "I'm giving my adversary easy intelligence"

While many organizations may view transparency as giving away too much intelligence to adversaries, transparency should be viewed as "the great equalizer" [9]. In cybersecurity, a common assumption is that an adversary intent on compromising an organization already has information about their installed digital assets through intelligence gathering, reconnaissance activities, and reverse engineering. In fact, the adversary may know more about the assets than the asset owner. Acquiring or generating SBOMs for digital assets installed in NPPs essentially "levels the playing field" between adversary and defender.

Therefore, since it is assumed the adversary has or can readily acquire SBOM data, it is important for NPPs to have the same information, or the "list of ingredients," for all their critical digital assets (CDAs), regardless of whether they are in-house, engineered, or commercial-off-the-shelf assets. Providing software transparency can reduce adverse impacts from an adversary by providing visibility into digital asset vulnerabilities and enabling faster mitigation and improved incident response. SBOMs linked with vulnerability information enable NPPs to understand, prioritize, and mitigate the most critical vulnerabilities in their systems—key elements of minimizing cyber risk. Additionally, the use of SBOMs during software development can improve efficiencies and provide greater insight into build and source components, as well as product functionality, for both the developer and user [10].

While adversaries may already have knowledge about critical systems and/or CDAs in an NPP, it is important to note that SBOMs should still be maintained and protected in accordance with the NPP's security requirements. Implementing an SBOM program is intended to provide greater transparency to the NPP to improve their security posture; it is not intended to provide an adversary easy access to the data. Additionally, the NPP will likely be required to maintain confidentiality and intellectual property rights as defined by the supplier procurement agreement or contract (refer to Section 3.1.8). The NPP should also ensure that the supplier is protecting the confidentiality and integrity of the SBOM to make sure the adversary does not have easy access to open-source intelligence.

2.1.5 Standards for SBOM formats

Using the baseline data fields defined in Section 2.1.2, a standard format should be used to structure the SBOM. Several standard SBOM formats exist, including CycloneDX [11], Software Package Data Exchange (SPDX) [12] , and SWID [13]. All three standards capture similar information and can be used for SBOM generation, ingestion, and use. This report does not recommend one format over another and leaves it up to the NPP to determine the best format for their purposes.

CycloneDX is a lightweight SBOM standard intended for use in application security and supply chain component analysis that began in the Open Web Application Security Project (OWASP) community [11]. It natively supports component identity standards, such as PURL, CPE, and SWID, and can be used for both open-source and proprietary software. There is ongoing work to develop and support open-source tools to enable automation and ease of use.

SPDX is an international open standard for SBOM security, license compliance, and supply chain artifacts that began in the Linux Foundation [12]. SPDX can link with CPE, PURL, and SWHID, enabling users the ability to freely generate SBOMs with little effort. The open-source tools can be used with both open-source and proprietary software to support SBOM generation and ingestion for software transparency.

SWID is defined by ISO/IEC 19770-2:2015 as a specification for tagging software for optimization of identification and management [13]. It supports both open-source and proprietary software and can be used for automatic tag generation during software processes and automatic scanning after deployment for

inventory management as well as other applications. While SWID remains an SBOM standard, there are fewer commercial and open-source tools that use it when compared to CycloneDX and SPDX.

2.1.6 SBOM ecosystem tooling

The number of software components used in in an NPP's OT environment will vary depending on the device and system. For instance, a smart transmitter will have fewer software components than a PLC, which will have far fewer components than a feedwater control system. These large numbers of components are often highly interdependent. In fact, SBOM databases are generally graph-based or tree databases instead of traditional hierarchal databases due to these complex interdependencies. A simple, notional graph database is shown in Figure 1 where C is subcomponent of B and D, similar to how an open-source library may be used in multiple software components.

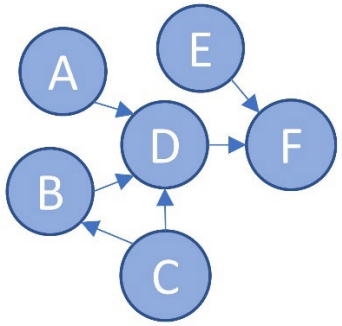

Figure 1. A simple, notional SBOM graph database, where C is a subcomponent used in both B and D.

Using a standard, machine-readable format provides capabilities to move towards automated SBOM generation and the use of other integrated tools as described in Table 4. Since the depth and breadth of content is often a challenge for manual SBOM creation, using automated or semi-automated tools to create SBOMs will drive efficiencies and completeness. It is important to note that the capability to use fully automated SBOM generation tools is more likely to occur during product development. NPPs will likely require a human-in-the-loop for enumeration of digital assets that do not have a supplier-provided SBOM or that are not custom developed by the NPP.

There are many SBOM tools available from both open-source and commercial developers. These tools may use techniques such as software composition analysis or binary composition analysis to generate SBOMs and can be categorized based on function, stage of use (e.g., during development, after procurement), level of automation (e.g., manual, semi-automated, automated), and format used (e.g., SPDX, CycloneDX, SWID).

NTIA describes the following functions for the SBOM tooling ecosystem [6]:

1. Produce an SBOM (e.g., automatically as part of the software build process, manually, or as an audit tool)
2. Consume an SBOM (e.g., enable viewing or human readability, provide difference comparisons, analyze and/or ingest/import into other software or tools)
3. Transform an SBOM (e.g., translate to another file type, merge data, integrate into tools such as APIs or libraries)

While an NPP developing custom, in-house applications may want to consider tools that produce SBOMs during their build processes, it is likely that most NPPs will require tools that can enumerate, consume, and transform SBOMs after the digital asset is procured. However, it should be noted that

SBOMs generated from source code are likely more complete than SBOMs generated from compiled code; therefore, legacy software that can only be analyzed using compiled or object code may have incomplete component and dependency listings.

Since capabilities in the SBOM tooling ecosystem are still evolving and the product marketplace is continuously changing, the most current registered product listings for each standard are available directly from the standards organizations as indicated in Table 5. Additionally, the Learn SBOM organization provides analysis and tool demonstration videos to assist NPPs in gaining further insight into generator, scanner and manager tools available in the SBOM ecosystem [14].

Table 5. SBOM tooling resources.

Standard	Resources
SPDX	The Linux Foundation maintains listings of open source [15] and commercial tools [16] that support the SPDX standard
CycloneDX	CycloneDX maintains a list of open source and commercial tools supporting their standard [17]
SWID	NIST maintains a list of SWID tools produced by the NIST SWID Tagging Project [18]

It is also important to note that vendor provided SBOMs might be incomplete or may not provide the depth, format, or dependencies desired by the NPP. Since these limitations may pose challenges to full interoperability with other tools in the ecosystem, an NPP should develop a plan for addressing this possibility.

2.2 Use Case—Vulnerability Management

Figure 2 illustrates proposed process steps for integrated SBOM vulnerability management analysis. Once components and subcomponents are identified in an SBOM (Step 1), known vulnerability data (Step 2) and vendor vulnerability attestations (Step 3) can be correlated to identify installed components with vulnerabilities (Step 4). Cyber risk management processes (e.g., analyze, prioritize, mitigate) can then be used to reduce risk (Step 5).

2.2.1 Vulnerability sources (Step 2)

Known vulnerability data is available through various sources, including vendor notifications, third-party notifications, and data repositories, such as Common Vulnerabilities and Exposures (CVE) and the National Vulnerability Database (NVD). CVE is a tool developed by MITRE that provides publicly disclosed information on security vulnerabilities and exposures that can link vulnerability data with other tools [19]. Conversely, NVD is a U.S. Government repository of vulnerability management data that is represented by using the Security Content Automation Protocol (SCAP) [20]. NVD data includes security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

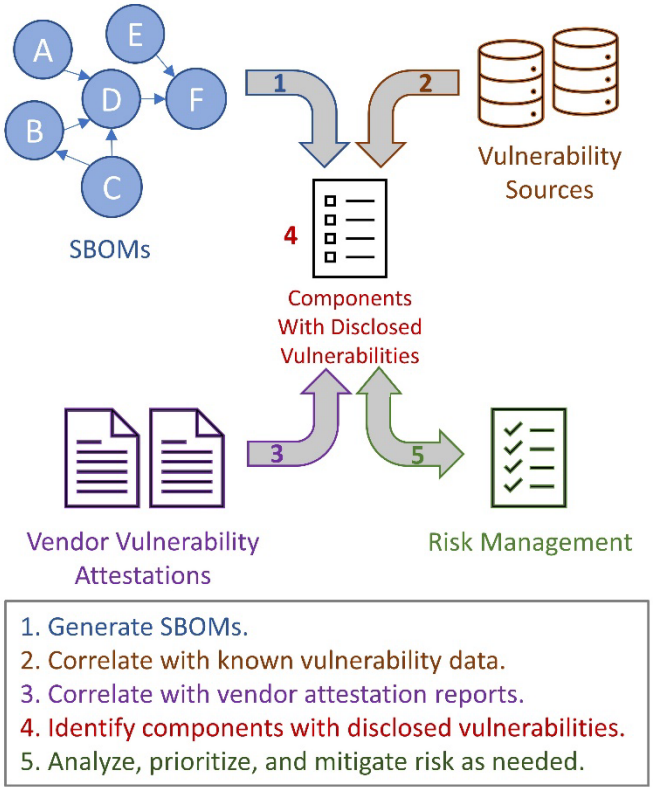

Figure 2. Process steps for integrated SBOM vulnerability management analysis.

2.2.2 Vendor vulnerability attestations (Step 3)

Vendor vulnerability attestations are security advisory reports provided by a vendor that assert the status of a specific vulnerability or vulnerabilities in their product(s). Although this space is very new and rapidly evolving, the VEX Working Group, started by NTIA and continued by CISA, has proposed the use of a Vulnerability Exploitability eXchange (VEX) document [21]. As described by CISA, the VEX model is an improvement over "traditional" security advisories since the documents are machine readable and can support greater automation and integration with SBOMs and other tools in the SBOM ecosystem, including disclosure, vulnerability tracking, and remediation [21].

A VEX document can be issued for a single product with a single vulnerability, a single product with multiple vulnerabilities, multiple products with a single vulnerability, and multiple products with multiple vulnerabilities [21]. Additionally, while useful as a companion artifact in the SBOM tooling ecosystem, they are also used as standalone documents.

Ideally, minimum data elements for vendor vulnerability attestations will include software component identification to cross reference to SBOMs and vulnerability details to known vulnerabilities. As listed in Table 6, the VEX model includes a status to describe the vendors research and response to a known vulnerability.

Table 6. VEX status definitions from [21].

Status	Description
Affected	Actions are recommended to remediate or address this vulnerability. [NOTE: VEX document must have an action statement telling the product user what to do.]
Not Affected	No remediation is required regarding this vulnerability. [NOTE: VEX document must have impact statement to further explain details.]
Fixed	These product versions contain a fix for the vulnerability.
Under Investigation	It is not yet known whether these product versions are affected by the vulnerability. An update will be provided in a later release.

2.2.3 Data correlation (Step 4)

Combining SBOMs with known vulnerability data and vendor vulnerability attestation reports can provide detailed insights into potential vulnerabilities associated with an NPP's digital assets at the software component and subcomponent levels. Since the volume of data in the SBOM ecosystem is extensive, automated or semi-automated tools can reduce the effort needed to maintain and correlate this data. Tooling may also provide quick visualization of vulnerabilities and their status associated with a given software component. Further, even though SBOMs in an NPP will be static unless a modification or update is performed, new vulnerabilities are continuously discovered and vulnerability details frequently change. Although not all vulnerability data is available through these sources, adding automation capabilities, when possible, can enable periodic (or continuous) scanning of vulnerability information.

2.2.4 Cyber risk management (Step 5)

However, although integrated SBOM tools provide detailed information about potential vulnerabilities in an NPP, a human-in-the-loop is still necessary to identify the vulnerability significance and its potential impact to the plant if remediation is delayed or not performed. This requires research into the vulnerability and how the asset is used and installed in the NPP. For example, existing security controls may significantly reduce the significance of a vulnerability. Thus, NPP risk management processes are required to further analyze and prioritize the risk in order to determine a risk treatment.

Cyber risk analysis considers threats, vulnerabilities, and consequences. Consider implementation of an integrated SBOM-vulnerability management process at an NPP which integrates SBOMs with vulnerability data and vendor vulnerability attestations. The following can be used for cyber risk analysis:

- Threats—defined by the NPP's design basis threat (DBT) and updated by threat bulletins or site experts
- Vulnerabilities—identified through the SBOM-linked vulnerability management process and compared with existing cybersecurity controls (e.g., a vulnerability may have a lower severity on digital asset located behind a data diode than one located on the other side)
- Consequence—identified through the CDA assessment process (e.g., impacts safety, important-to-safety, security, emergency preparedness, or other support equipment)

While it is likely that an NPP will not have complete SBOMs for all CDAs and that many subcomponents will not have vulnerability data and/or vendor vulnerability attestations, it is still anticipated that implementation of this process will provide key insights into the cyber risk associated with CDA threats

and vulnerabilities, thereby enabling the NPP to make risk-informed decisions on risk treatments and mitigations. Further research is necessary to support this claim.

2.2.5 Additional considerations

The VEX model and vendor vulnerability attestation reports are still new and unproven. Similarly, tools to support these reports in the SBOM ecosystem is still ongoing. Additionally, these reports may be updated and tracked independently of SBOMs or they may be embedded in SBOMs, depending on the functionality required. Further, existing VEX tools may be open source or commercial. The sources listed in Table 5 can be used to identify the current listings of VEX tools that are interoperable with a specific SBOM standard.

Of course, storage requirements for all the data in within the entire SBOM ecosystem must be considered, especially when recognizing that an NPP may have thousands of digital assets. Understanding the security classification of the data and the relevant NPP security storage requirements may drive tool selection decisions.

2.3 SBOM Industry Activities, Regulations, and Standards

While the concept of SBOMs has existed for decades, the increasing prevalence of software supply chain attacks and expanding frequency of open-source and third-party components in software has more recently resulted in industry and government groups directing efforts towards establishing software transparency to reduce cyber risks. In 2018, NTIA established a Multistakeholder Process on Software Component Transparency to develop common consensus definitions for SBOM. In May 2021, the Office of the President issued EO 14028, Improving the Nation's Cybersecurity, establishing specific requirements for U.S. government acquirers in response to the SolarWinds supply chain attack [4]. Among other requirements, Section 4 of EO 14028 directed NTIA to establish minimum elements for an SBOM and instructed NIST to issue standards and guidance to enhance software supply chain security by providing criteria to secure the development environment, establish software integrity and provenance, and provide an SBOM to purchasers for each product [4]. As identified in section 2.1.2, NTIA completed the work of establishing minimum elements for an SBOM.

In addition to NIST's website dedicated to EO 14028 [22], NIST provides additional cybersecurity supply chain management practices in SP 800-161r1 [23] and recommendations for mitigating software vulnerabilities in SP 800-218 [24]. Similar to the "crawl, walk, run" approach, NIST specifies SBOM capabilities as either foundational, sustaining, or enhancing [22]. As NIST continues working on EO 14028, it is anticipated additional guidance on SBOMs will be forthcoming.

Many SBOM initiatives are underway. NTIA [25] and CISA [26] have numerous resources on their websites. In 2018, CISA established the information and communications technology (ICT) SCRM Task Force as a public-private partnership to identify and develop C-SCRM strategies [27]. In 2022, this Task Force created two working groups—a software assurance and a hardware BOM working group—to enhance supply chain resilience. While this Task Force is focused on ICT, the awareness materials provided on the website are also applicable to OT products. It is anticipated that the task force will release new SBOM materials within the next year. DOE-CESER is also collaborating with CISA and a group of diverse energy-sector stakeholders to explore application of SBOMs within the Energy sector in order to drive SBOM adoption [28].

As described in Section 2.1.5, several standards exist for SBOM formats, including OWASP CycloneDX [11], Linux Foundation SPDX [12], and ISO/IEC SWID [13]. Additionally, OASIS released CSAF 2.0, which is a language to exchange security advisors formulated in JSON [29]. CSAF enables VEX as a profile to improve automation of security advisories and integration with SBOM tools.

Additionally, the DOE Office of Nuclear Energy Cybersecurity Program plans to continue research and development into SBOMs and their integration with other governmental and industry efforts, such as the DOE's National Strategy for Cyber-Informed Engineering [30, 31], Electric Power Research Institute's Digital Engineering Guide [32] and/or Cyber Security Technical Assessment Methodology [33], and the Nuclear Energy Institute's cybersecurity efforts.

Notwithstanding government and standards activities, many suppliers are researching and updating tools for automating and improving the SBOM generation and vulnerability management process. While the potential options may seem overwhelming, it is important to recognize that implementing an SBOM is a process that can move at a pace determined by the NPP, depending on resources available. The most important step is to start.

3. RECOMMENDATIONS FOR INTEGRATING AN SBOM PROGRAM INTO AN NPP

Integrating an SBOM program into an existing NPP is a long-term process, especially since it is likely that most of the installed digital assets can only be analyzed during outages. The steps in these sections are meant as a guide to tailor a project as needed. The intent is to integrate an SBOM program into an NPP using existing resources with limited additional funding or personnel, recognizing that if it cannot be accomplished with the existing operating and maintenance (O&M) budget, then there is low likelihood for project success in the current NPP fleet. A benefit, however, is that successful implementation of an SBOM program will simplify risk and vulnerability management, which may reduce O&M costs over the long-term.

The functional objectives for the project are to:

- use existing personnel,
- simplify current plant processes,
- integrate into existing programs and workflows (e.g., cybersecurity, asset and configuration management, engineering change, digital engineering, supply chain),
- establish semi-automated and periodic (or continuous) vulnerability management, and
- reduce overall cyber risk to improve the security posture of the NPP.

Implementing an SBOM program at an industrial facility, including an NPP, is an immature process, especially since tooling and integration concepts are still being researched and developed. However, even though implementing a program that captures every SBOM for each digital asset installed in an NPP seems daunting, the first step is to start the program. Even if it is a slow process to capture SBOMs, each step will enhance software transparency, improve response to new threats, and reduce overall cyber risk.

Suggested activities for each stage of the "crawl, walk, run" SBOM project are listed in Table 7. In the 'crawl' phase, foundational activities will lay the groundwork for the program. It is likely the first SBOMs will be acquired from suppliers during the procurement process. In the "walk" phase, sustaining activities will result in establishment of tools and repositories such that enumerating SBOMs of installed equipment is possible. Integration with vulnerability data and correlation tools will begin to provide actionable vulnerability information. And finally, in the "run" phase, enhancing activities will establish automation tools for enhanced monitoring of vulnerabilities and seamless integration with other NPP programs.

The order of activities in each phase is a recommendation. An NPP may choose to move an activity up or down depending on their overall project timeline and resource availability.

Table 7. Recommended SBOM project activities for each "crawl, walk, run" phase.

Phase	Section	Activity
CRAWL (foundational)	3.1.1	Develop a project plan and change management plan
	3.1.2	Determine project roles and responsibilities
	3.1.3	Identify existing programs and workflow changes
	3.1.4	Determine SBOM format and minimum requirements
	3.1.5	Identify repository and security requirements
	3.1.6	Identify tooling requirements
	3.1.7	Create SBOM documentation
	3.1.8	Update procurement procedures
	3.1.9	Identify other policy and procedure changes
	3.1.10	Prioritize digital assets and develop SBOM generation schedule
	3.1.11	Acquire available SBOMs and vulnerability information
	3.1.12	Run a pilot test
WALK (sustaining)	3.2.1	Establish/acquire SBOM tooling
	3.2.2	Establish or enhance SBOM repository
	3.2.3	Generate and maintain SBOMs
	3.2.4	Establish or enhance vulnerability tracking
	3.2.5	Establish vulnerability incident response process
RUN (enhancing)	3.3.1	Integrate into existing NPP programs and processes
	3.3.2	Develop capabilities to dynamically monitor SBOM vulnerabilities
	3.3.3	Establish/enhance a secured, central repository for all data
	3.3.4	Complete SBOM generation for all installed digital assets
	3.3.5	Maintain awareness of ongoing industry advancements

3.1 Crawl–SBOM Foundational Activities

While it may seem ambitious to develop and implement a full-scope, automated SBOM program for every digital asset installed at an NPP, the goal is to start slowly and gradually build the program over time. Since NPPs have both limited budgets and limited availability of qualified individuals, the intent of this guide is to establish methods that enable development of the program using existing resources. As the

project matures and tool automation is implemented, it is anticipated that resources needed for existing processes, such as continuous monitoring, vulnerability management, and risk management, will decrease, thereby offsetting or reducing overall costs.

3.1.1 Develop a project plan and change management plan

As with any project, the first step in implementing an SBOM program is to develop the project plan. Suggested project activities are listed in Table 7. The project timeline depends on resource availability and NPP priorities—the ability to remain agile as new advancements occur or challenges arise is key to successful implementation. NPPs with available, qualified personnel and sufficient budget may develop a more aggressive timeline when compared with an NPP implementing the program using existing resources.

While developing the project plan, also identify requirements for the change management plan. Successful organizational changes require careful planning to ensure all stakeholders are onboard with the new processes. Communicate early and often the planned process changes and the anticipated implementation timelines. Highlight the benefits of the new SBOM program, including improved transparency, risk management, and cybersecurity.

3.1.2 Determine project roles and responsibilities

Based upon the project plan, identify the roles and responsibilities for the project. If the intent is to slowly roll out the project using existing resources, considerations should include the knowledge, skills, and abilities of current personnel to identify who can support the project with their current workload. Ongoing programmatic roles and responsibilities are identified in Section 3.1.7.

At minimum, the project team should include a Management Sponsor, Project Lead, Systems Engineer, Design Engineer, Procurement Specialist, and Operations representative. Ancillary support may include maintenance, plant and/or corporate IT, additional cybersecurity specialists, design and/or systems engineers or personnel, and procedure writers. Vendor support for any commercially acquired tools may also be needed during certain stages of the project. Additionally, the plant's Cybersecurity Assessment Team (CSAT) should be involved or informed for the duration of the project. Individuals may overlap as members of both the CSAT and the project. The number of personnel on the project depends on the timeline—a more aggressive timeline may require more project personnel, while a longer timeline may be able to minimize the number of personnel involved.

To ensure the success of the plan, a Management Sponsor should be enlisted to promote and support the project. Typically, the Project Lead is a Cybersecurity Specialist with experience in implementing or maintaining the plant's cybersecurity plan. The Project Lead should have knowledge of the plant's digital assets and be able to interact with plant engineers and operations personnel to assess and prioritize the SBOM generation schedule. They will likely need training on various aspects of the SBOM ecosystem, both prior to and during the project. A Procurement Specialist should be included to assist with updating procurement policies and procedures to require inclusion of an SBOM in contracts or specifications used for procuring and repairing digital assets.

A Systems Engineering representative should be included to provide overall support for the project. Additional Systems Engineers who are responsible for an installed digital asset may also be required to provide specific, but likely intermittent, support as the asset is evaluated for inclusion in the SBOM program and as its SBOM is generated. A Design Engineer should be included on the initial project team to assist with inclusion of SBOM program requirements into new digital engineering changes or modifications and to ensure that in-progress digital modifications mandate inclusion of an SBOM as a project deliverable. Additional Cybersecurity Specialists or Systems Engineers who support the

cybersecurity program will likely be necessary on an interim basis, depending on plant requirements and project timeframe.

Similar to inclusion in the CSAT, operations, maintenance, and planning representatives are necessary to understand the plant impact when enumerating the SBOM of an operational digital asset (i.e., does the digital asset need to be out-of-service and, if so, what are the operational impacts?). They will also be necessary for scheduling the activity within the work management program. With business-facing assets, such as boundary devices to the business network, plant or corporate IT staff may be necessary to assist with SBOM generation. Procedure writers may be necessary to update policies and procedures to incorporate SBOM activities into current programs and practices.

3.1.3 Identify existing programs and workflow changes

To identify necessary site-level changes impacted by the SBOM program, first identify all programs and/or workflows that include digital assets. Next, narrow the list of programs to those directly or indirectly affected by SBOMs. For instance, an SBOM program is an integral part of the Cybersecurity Program since the SBOM program's primary goal is to improve the transparency of components within installed digital assets to improve the overall security posture.

The SBOM program should be integrated with the Digital Engineering Change/Modification program and the Asset and Configuration Management program to clearly identify the need to capture the SBOM of digital assets as new systems or assets are installed or as existing systems are modified. Engineering Change and Configuration Management procedures should be updated to require that new SBOMs are generated with any software change or update, including custom or in-house developed software as well as commercially procured assets. SBOMs are just as important for custom software since custom development often relies on other commercial or open-source components and subcomponents, such as libraries. In-progress engineering change packages should be updated, as possible, to require SBOMs for all digital assets impacted in the modification.

Proper update and storage of SBOMs will assist with capturing the as-found configuration of the plant. Since an NPP will already have digital asset and CDA lists along with relevant configuration information in an Asset Management program, it is important to identify how this information can be used and/or integrated between the programs. Additionally, it may also be possible to integrate the ongoing monitoring of SBOMs into Preventive Maintenance (PM) and/or other cybersecurity activities to help ensure SBOMs remain up to date.

The SBOM program can also be integrated with Risk Management and Supply Chain programs. As discussed, risk management is the process of identifying, prioritizing, and treating risks. When combined with the Cybersecurity and SBOM programs, the enhanced transparency enables the Risk Management program to more proactively identify threats, vulnerabilities, and consequences in order to apply mitigations in both a graded and timely approach. Linking the SBOM with vulnerability data and vendor vulnerability attestation reports will help cyber risk analysts prioritize newly identified vulnerabilities based on existing security controls and potential consequences to determine a risk mitigation strategy. For example, software component vulnerabilities that have lower consequences as determined by risk analysis will have lower mitigation priority, while assets with high consequence vulnerabilities should be mitigated first.

Similarly, SBOM and Supply Chain programs are tightly integrated. The complex, global supply chain has resulted in better availability, improved efficiencies, and new innovations, while also expanding the cyber supply chain attack surface with multiple-tiered suppliers and related stakeholders. Enumerating the SBOM of a digital asset provides an enhanced understanding of these touchpoints by incorporating the provenance and pedigree of the products. The enhanced capability obtained by enumerating the levels and components in a digital asset provide a better understanding of product quality, security, and risk.

3.1.4 Determine SBOM format and minimum requirements

As identified in Section 2.1.5, there are several standard SBOM formats (e.g., CycloneDX, SPDX, SWID) that can be used for SBOM generation, ingestion, and use. As a part of developing the SBOM program, the NPP should decide on which format to use. The NPP should stay consistent with the format chosen while enumerating installed components. Similarly, if possible, the NPP should require that suppliers provide the SBOM in the chosen standard format. Prior to selecting the format, it is suggested that the NPP consider additional tools that will be used and to poll current suppliers to identify if one format is preferred over another. Since all formats are acceptable for use and since tools are available to convert one format to another, the primary goal for this step is to standardize a format for the NPP.

Additionally, the NPP should determine the minimum elements required for the SBOM. While it is likely that not all data fields will be available for every SBOM, the minimum fields and practices (e.g., depth, frequency, completeness) should be established. It is strongly recommended to use PURL (or similar) conventions for uniquely identifying each component.

As mentioned, a vendor may only provide a partial SBOM. The NPP must identify what steps they will take, if any, to acquire a full SBOM for the asset. Furthermore, since accuracy and completeness are both important, the NPP should identify methods to validate and verify acquired SBOMs.

3.1.5 Identify repository and security requirements

Consider the project and timeline for planned automation and support. Since SBOM information is likely considered security-related information (SRI), it should be protected in accordance with site security policies and procedures. Safeguards-related information has even more restrictive security and storage requirements, so care must be taken to properly classify the information.

Initially, the individual SBOMs may be stored in a segregated repository. As the project continues, SBOM information for each asset may be linked with asset management applications via the equipment ID. Later, there may be additional linked tools and applications, such as vulnerability data and vendor vulnerability attestation reports, that will also require secure storage.

Depending on capabilities and security requirements, acceptable storage locations may be the site business LAN, physical storage devices in an isolated, secured onsite location (e.g., for safeguards information), or in a secure cloud repository. Although dependent onsite security requirements, the use of electronic storage will more easily enable future integration with additional tools.

Additionally, the NPP should identify what process will be used to audit storage and/or custody. At minimum, a registry should record the date and version of files, and all access to the repository should be controlled using plant security requirements along with auditable access logs. Any contractual security requirements from suppliers or other entities should also be enforced.

3.1.6 Identify tooling requirements

The tooling choices an NPP will make are likely dependent on its size and the available resources. For instance, smaller NPPs with lower budgets may choose to have more manual processes and tools for the collection and storage of SBOM data. Additionally, since smaller NPPs will have fewer components needing documented and changes may occur less frequently, a manual process may be a less expensive and more sustainable method. However, semi-automated and automated processes are preferred.

Conversely, larger NPPs and/or NPPs with higher budgets will likely want to incorporate as much automation into their SBOM data gathering processes as possible. Larger NPPs are likely to have

constantly changing components, with an SBOM needing constant attention. Intuitively, as the level of SBOM automation increases, the level of manual intervention to maintain an SBOM up-to-date decreases.

As an NPP researches the most suitable processes and tools to use for their SBOM program, there are several questions to consider while reviewing Section 2:

1. What tools will be acquired or developed (i.e., what is the extent of the SBOM program)?
2. How will the tools be acquired (e.g., in-house developed, open source, commercially available, or a combination)? If custom developed, are resources available?
3. Does the tool support the preferred SBOM format (refer to Section 3.1.4)? If not, what is needed to convert the data to the required format?
4. What discovery processes should the tool(s) use?
    a. If discovery processes are via the network, can the OT infrastructure support it? If not, are there alternatives? Can network discovery be used in offline activities or during outages when equipment is not required?
    b. Should the process be automatic, semi-automatic, or manual?
    c. What type of analysis is preferred? For example, software component analysis, binary code analysis, or other SBOM enumeration.
    d. To what depth can the tool analyze? Are all subassemblies and/or subcomponents analyzed? Is the depth adequate?
5. Where is the tool located/maintained (refer to Section 3.1.5)?
    a. Is this location in compliance with NPP security requirements?
    b. If off-site, does the supplier maintain appropriate physical and electronic/cyber security? Do they have third-party attestation of their security practices?
    c. What are the communication channels? Is the channel security in compliance with requirements?
6. What is the interoperability of the tool(s) with other processes, programs, and/or data sources (e.g., vulnerability management, nonconformance/defect data, asset management, risk management, supply chain)?
    a. Is the integration automatic, semi-automatic, or manual?
    b. What is the volume and granularity of data? Ensure workflows can scale to the data.
    c. Does an interface exist (commercial or open source) for the SBOM, or will it need to be custom developed? What is the data feed into the workflow? How is the data ingested? What does the data mapping look like? Does it use the standard format? Does the data need to be parsed, extracted, or loaded into automated or manual processes? Are dependencies considered?
    d. How is the integration validated and verified? Are there digital signatures or hashes?
7. How is entity resolution handled? There are often name-space issues with vendors, manufacturers, and product lines. How is disambiguation and specificity ensured? Consider that SBOMs generated outside of the software build process may be more arbitrary.
8. What ongoing/continuous monitoring is available with the tool(s)? For example, how often does a commercial tool update their product/component vulnerability data?

3.1.7 Create SBOM documentation

As necessary for the NPP, create SBOM documentation, which may include a high-level policy document or only SBOM-related procedures. Depending on existing policies and procedures, it may be possible to integrate this material into existing documentation. Unless required by the NPP, modification of the Cyber Security Plan is unnecessary. Additionally, while this report refers to an SBOM program, the designation of "program" at an NPP may result in additional requirements depending on the facility. It is left up to the NPP to determine how best to identify their SBOM implementation; simply eliminating the word "program" may be satisfactory.

Documented policies are important for defining the roles and responsibilities of staff associated with the SBOM tool, the scope of what the tool is used for, and how to accomplish the goals around the SBOM. It's important to keep these documents up to date. The following elements are recommended in the SBOM documentation:

1. Overall SBOM program description, goals, and objectives. Define why the SBOM program exists in the NPP. What is achieved by deploying this tool? What processes does this program support and how does the program accomplish these goals?
2. Scope. Define the breadth of the SBOM program as well as all components used to meet the defined purpose.
3. SBOM ecosystem requirements, as identified throughout Section 3.1:
    - Roles. What are the organizational roles? Who owns the system? Who operates the systems? Who has dependencies on the system?
    - Responsibilities. Along with the defined roles, what are the responsibilities of those roles as they relate to the SBOM ecosystem?
    - Management Commitment. Management should indicate in the policies their commitment to operating the SBOM tool(s) and express their intent to keeping the tool(s) operational by dedicating the necessary resources to maintaining and enhancing its use.
    - Compliance: Identify regulatory requirements, laws, standards, and orders that the SBOM program supports, if any. If the SBOM program is non-functional, what are the impacts from a regulatory perspective, if any.
    - Program and workflow integrations. Identify other entities, programs, or workflows that are dependencies or are dependent of the SBOM program. Where does SBOM information come from? What processes rely on SBOM data?
    - SBOM format and minimum requirements.
    - Repository and security requirements.
    - Procurement requirements.
4. Identify the retention policy, archival storage requirements, and how long SBOMs should be maintained after asset disposal or decommissioning.
5. Contingency and incident response plans for following situations:
    - Contingency plan for incomplete (e.g., components improperly identified) or inaccurate (e.g., components identified that are not present) SBOM enumerations?
    - Contingency plan if vulnerability information and/or vendor vulnerability attestation report updates are not timely?
    - Response plan if a component supplier is slow to develop and/or release a fix for an identified vulnerability? Will the NPP accept remediations in the vulnerability reports instead of eliminating the vulnerability?

These procedures establish the standard by which the program should be operated and utilized. They should be detailed enough for new team members or program leads to follow without an adverse impact to program operation.

3.1.8 Update procurement procedures

While many processes and procedures may need to be updated for proper integration of the SBOM program into an NPP, procurement procedures for digital assets should be updated first. Acquiring an SBOM as part of the procurement process shifts the level of effort to the supplier, which reduces the overall resources required for the program. While not guaranteed, if SBOM enumeration is performed by the supplier as part of software development, the SBOM may have greater depth and accuracy than those created after installation. In any case, it is easier to generate the SBOM prior to installation.

Thus, procurement policies and procedures should be updated during the "crawl" phase to require the supplier to provide an SBOM as part of the purchase order, agreement, contract, and/or other procurement documents. Although not federally mandated, suppliers should not be surprised when an end user in a critical industry requests an SBOM [4]. The following additions to the procurement terms and conditions are recommended:

- Delivery timeframe of SBOM (e.g., upon order, prior to delivery, on delivery, and/or on product update).
- Specification of SBOM elements (refer to Table 1), including but not limited to format, data fields, depth, update frequency (with precise versioning), and identification of known unknowns.
- Enumeration of all components (e.g., commercial, custom, open-source, third-party components and dependencies); run-time dependencies (e.g., dependencies installed by compilers and download managers); components enabling a capability; and components in containers. This should include supply chain provenance and pedigree, including chain of custody. [NOTE: the acquirer should understand software origin and whether it is from uncompiled open-source code, binary packages created with a package manager that includes runtime dependencies, or containers that may include many additional components, such as operating systems, in addition to the payload. Depending on the source, undefined components may exist in the final delivered product. Further, since it is difficult to map vulnerabilities to higher-level packages, there is often less transparency (and higher risk) with these products.]
- Delivery method for the SBOM, which may be in a physical format (e.g., USB, CD-ROM), electronic delivery (e.g., email), or cloud repository download (e.g., customer portal). The security measures to ensure appropriate protection against compromise must also be specified.
- Rights for acquirer to (1) reverse engineer a binary and (2) compare against the provided SBOM.
- Rights for acquirer to investigate and resolve any discrepancies.
- Confidentiality and intellectual property requirements, including non-disclosure agreements of the SBOM itself (in addition to any software requirements). The NPP should have the rights to use the SBOM internally, including onsite contractors, without seat licensing limitations.

If the supplier or contractor cannot provide an SBOM, then the procurement and receipt inspection procedures should allow for (and require) SBOM generation for the digital asset upon delivery (assuming the in-house SBOM tool is available). Additionally, if possible, SBOM procurement language should be added to existing and in-progress purchase orders, agreements, and contracts.

Note that SBOMs are generally unavailable for open-source software. Upon receipt of the digital asset, the acquirer can generate the SBOM from the repository or build procedures. The acquirer must verify integrity, provenance, pedigree, and trustworthiness upon receipt.

3.1.9 Identify other policy and procedure changes

In addition to procurement policies and procedures, other policies and procedures may be affected by the SBOM program. Starting with the program and workflow analysis, the Project Lead or designee should develop a "procedure update" list that is prioritized by criticality to the program. This list should indicate when each procedure should be updated. For instance, it may be identified that a specific digital engineering modification procedure should be updated early in the project in order to require all modifications (in-progress and future) to require SBOM generation for any digital assets prior to installation and/or operation, while a lesser impacted procedure can be updated later in the project during the "run" phase.

3.1.10 Prioritize digital assets and develop SBOM generation schedule

NPPs should consider overall system risk when developing the SBOM generation schedule. Systems that pose more risk to an NPP should be prioritized first. As part of their Cyber Security Plan, U.S. NPPs have identified critical systems and CDAs—those digital assets that, if compromised, could impact safety, important-to-safety, security, emergency preparedness, or supporting equipment. Since critical systems are more likely to impact the health and safety of the public, it is preferred to capture their SBOM prior to other systems. By prioritizing these systems above others, an NPP stands to benefit more by having partially completed systems than if generating SBOMs for less critical systems first. For example, the details provided in an SBOM can accelerate the performance of cybersecurity activities, such as vulnerability management and incident response. The ability to respond in a timely manner could prevent (or rapidly detect) the potential (or actual) adverse impact of a critical function.

However, while it is desired to gather SBOM information from CDAs first, it may be impossible to enumerate the SBOMs of many CDAs while the plant is operating as the activity may adversely impact plant operations. Therefore, the prioritization list and SBOM generation schedule must also consider plant modes and the capability for online enumeration of each CDA. Additionally, the NPP may want to place CDAs with fewer security controls or defense in depth, or those that are external to the data diode, higher in the schedule.

The schedule should also consider the ability to generate SBOMs from like-digital assets (e.g., same make, model, and version) that are in a plant simulator, development environment, or warehouse inventory. If it can be guaranteed that the digital asset is the same make/model/version of the installed digital asset, then offline SBOM enumeration is possible, and the schedule should incorporate this capability into the prioritization list.

While CDAs should be prioritized higher than less critical assets, the schedule should also consider the ability to acquire SBOMs that are already available, either from the supplier or those digital assets that are already documented in existing asset configuration management repositories where information can be easily transferred to the new SBOM program. Capturing this "low hanging fruit" while waiting for schedule opportunities to enumerate installed digital assets can help shorten the overall project schedule. Of course, if a modification to an installed asset occurs, the SBOM should be generated as part of that change.

While enumerating SBOMs for CDAs is a high priority, other digital assets that do not impact the health and safety of the public but that do impact other NPP concerns, such as equipment operation or financial losses, should also be placed into the SBOM program. The schedule should continue to rank

digital assets based on risk priority and ease of SBOM acquisition. This schedule could include prioritize digital assets that can be enumerated online or that do not impact plant operations if taken offline. Of course, populating the SBOM repository with as much information as quickly as possible will benefit the NPP most.

Requirements for SBOM generation must be considered (e.g., offline vs online, plant mode, only during modification) when generating the remainder of the schedule. Since enumerating the SBOMs of many NPP digital assets may only be possible during outages, this process may take a long time to complete. Of course, as identified in Section 3.1.8, any new or modified digital assets should require SBOM generation as part of the engineering change process. There should be a continual effort throughout the life of the plant to ensure SBOMs are captured and documented appropriately for all installed digital assets.

3.1.11 Acquire available SBOMs and vulnerability information

As identified in Section 2.1.2, several factors will determine whether an SBOM is available for installed or legacy digital assets, including component age, product history, and supplier viability. However, it is possible that SBOMs have already been generated by suppliers for assets installed (or in inventory) at an NPP. NPPs should use their Asset Management program and equipment database, as well as digital asset and CDA lists, to identify the associated make/model/version of each digital asset. If the ability to acquire an SBOM directly from an installed digital asset (or like-digital asset) must wait until the system is offline or the plant is shutdown, then it is useful to determine whether the SBOM is available from the supplier. Since tooling may not yet be acquired in the "crawl" phase, acquiring readily available SBOMs from suppliers enables the project team to start populating the SBOM program. The project team should also verify the completeness and accuracy of acquired SBOMs, as identified in Section 3.1.4.

Similarly, the project team should acquire available vulnerability data and vendor vulnerability attestation reports during this step. An NPP should already have vulnerability information for their CDAs as part of their cybersecurity program so this information should also be gathered. While tools may not yet be in place to integrate SBOMs with this information, it is still helpful to obtain and store them at this stage.

It is important to note that the SBOM and vendor vulnerability attestation environment is rapidly changing. Thus, the project team should maintain awareness of ongoing industry programs. It is possible that a shared, central SBOM repository could be instantiated for the U.S. nuclear fleet, thereby enabling more efficient acquisition of SBOMs.

3.1.12 Run a pilot test

Once a tool is identified, it is beneficial to run a pilot test to verify that the tool operates as expected. A pilot is also a good technique to validate that plant processes and procedures are integrated and established correctly. If additional tools are developed or acquired during the project, a pilot test may be repeated, especially there is new interoperability with tools already implemented.

3.2 Walk–SBOM Sustaining Activities

3.2.1 Establish/acquire SBOM tooling

After tooling needs are determined in Section 3.1.6, it is necessary to identify the tools that best fit the NPP's needs in accordance with available budget requirements. Most SBOM tool vendors allow potential clients to test their product with a limited use license or Proof of Value evaluation of their products. This affords the interested party to test out the product's features and capabilities without committing to purchasing the product. It is best to compare multiple products' features and capabilities against each other to determine which product has the capabilities and features to best suit the NPP's expectations on how to operate and maintain and the SBOM program. It is important to note that purchasing a tool may not always be the best option. An in-house, custom tool may be more feasible. NPPs should consider all options.

Once evaluations are complete, the project team, along with management, should determine either:

- The tool(s) they will purchase, or
- The tool(s) they will develop in-house.

Whatever option is selected, the NPP should follow established plant processes to acquire or develop the new SBOM tool.

3.2.2 Establish or enhance SBOM repository

When new SBOM software is purchased, the vendor will often assist with the installation and initial configuration of the tool. It is incumbent on the project team to implement the minimum data fields determined in Section 3.1.4. If not already completed, procedures should be created to describe the various methods acceptable for populating the data fields. The procedures should be repeatable and easily understood by anyone new to the tool(s), including successive SBOM program administrators.

Any SBOMs that existed prior to instantiation of the repository should be migrated into the new storage location using the correct SBOM format and elements. Depending on formats and available tools, this migration process may be manual or automatic.

3.2.3 Generate and maintain SBOMs

SBOM, engineering change, and configuration management procedures and processes should be created or updated to provide instructions to plant personnel on how to incorporate digital asset software information into the new SBOM program. Depending on the SBOM generation tool acquired or developed, these instructions should specify the steps for enumerating an SBOM using the tool. Ideally, a pilot test was run to validate and verify the process and procedures.

Once the SBOM tools and repository infrastructure is in place, the project team should use the SBOM generation schedule developed in Section 3.1.10 to begin enumerating SBOMs of installed digital assets. Procedures should identify how to determine if a digital asset can be enumerated online or offline in the event the SBOM generation schedule is inaccurate. Operations should be informed of all activities performed on installed CDAs.

Generating SBOMs for all digital assets may take several years, based upon availability of the asset and outage schedules. The goal is to slowly and methodically use existing plant resources to create the SBOMs based on the prioritization list. While this process might be lengthy, every new SBOM that is

generated provides enhanced security and risk management capabilities. Of course, NPPs that have set aside additional resources may move faster and complete the project earlier.

SBOM, engineering change, and configuration management procedures and processes should be updated to require SBOM generation whenever existing digital assets are modified, or new digital assets are acquired and deployed in the NPP OT environment. Additionally, these procedures and processes should identify how to update the SBOM for digital assets when they are modified in the future. In the event an existing digital asset without an SBOM is modified, the engineering change package should require an SBOM, and the SBOM generation schedule should be updated to indicate its completion.

It is important for SBOM data to remain up to date. If an SBOM is outdated, it has less value to the NPP. If a vulnerability is identified and the SBOM is not current or is incomplete, plant personnel may not recognize that a vulnerability exists. Generally, an SBOM will only require updating if the asset is modified. It is important to recognize, however, that software patching or security updates may change the installed versions of components and subcomponents. Any updates that affect components or dependencies, no matter how deep, require a new SBOM, including updated timestamps, version information, unique identifiers, and/or hashes.

3.2.4 Establish or enhance vulnerability tracking

If not already implemented, the NPP should establish how they will track vulnerability data associated with the SBOMs. When implemented, the project team needs to ensure procedures are in place to identify any recurring tasks or preventive maintenance procedures to ensure these processes remain secure, functional, accurate, and trustworthy.

If the NPP has not yet implemented semi-automated or automated vulnerability tracking, then the manual vulnerability processes followed in the NPP's cybersecurity program should be integrated with the SBOM program. Since NPPs already have historical vulnerability information as part of their cybersecurity program, they should initially ensure this historical information is captured and maintained in the SBOM ecosystem. If the cybersecurity specialist receives a vendor notification about a vulnerability, a procedure should be in place for the specialist to search the SBOM repository and the equipment database configuration data to see if the identified product or component is found. This process of manually checking both repositories will become less onerous over time as SBOMs for all digital assets are generated.

3.2.5 Establish vulnerability incident response process

An SBOM program is a useful resource for a cybersecurity incident response team. Not only are product vulnerability reports available, but CISA and other proprietary cybersecurity threat analyst organizations will issue alerts or advisories on various threats. Often, these threats are associated with newly disclosed software vulnerabilities. Response teams and hunt teams use this information to determine if their organizations are vulnerable to the newly discovered threat and whether they have been compromised by it.

While completing the SBOM project implementation and having SBOMs available for all installed digital assets in an NPP makes searching for vulnerable components fast and simple, at this phase it is likely there are still assets not yet in the SBOM program. Therefore, the incident response process may need to be updated as the SBOM project continues.

Once the project is completed and the SBOM repository contains accurate and complete SBOMs for all digital assets in the plant, it is easier to respond to vulnerabilities. Newly discovered vulnerabilities for components not found in the SBOM repository are not a threat to the plant. For newly discovered

vulnerabilities in components that are in the repository, the incident response team should immediately follow their incident response procedure to determine if the vulnerability has been exploited and if the device is compromised. An SBOM repository can decrease incident response times, thereby improving the likelihood of delaying or stopping an attack, including preventing or interrupting initial adversarial access.

3.3 Run–SBOM Enhancing Activities

3.3.1 Integrate into existing NPP programs and processes

As the SBOM program is implemented in the "crawl" and "walk" phases, the program should be refined over time to ensure it operates as efficiently as possible. This section covers actions the project team can take to streamline the SBOM program operation and maintenance and to integrate it into other plant programs and processes in order to gain additional plant insights and efficiencies.

Procedures to address how the SBOM program is established, configured, and used should be developed as part of the "crawl" phase, as described in Section 3.1.7. Following normal NPP procedure revision processes, the SBOM procedures and any other related procedures that have been revised as part of the project should be updated as changes occur (e.g., policy changes, error discovery, new methodologies, tool updates, features added, or other program or procedure integrations). The NPP should follow their standard procedure review and update process to ensure the SBOM procedures and related procedures remain complete and correct over time.

As the SBOM program matures, integration with other existing plant programs and procedures, as identified in Sections 3.1.3 and 3.1.9, will provide enhanced benefits to the NPP. Consider also the SBOM use cases in Table 4. To fully recognize the benefit of SBOMs, the program can be used to provide more than just improved software inventories and vulnerability management. The project team should continually enhance the SBOM program to provide current software inventory in near real-time. To accomplish a real-time view of software installed in an NPP's OT environment, the standard format and machine-readability attributes of SBOMs enables integration into the NPPs asset management system with an added visualization tool to provide current SBOMs for digital assets. Upon changes to a digital asset's SBOM, the equipment database with linked SBOM can be automatically updated. Since software in an NPP is updated in a controlled manner using engineering change processes, it is anticipated that SBOMs will be changed infrequently. Of course, ensuring that the as-found SBOM data equals the as-built SBOM data is a foundational activity in ensuring an NPP's design basis is maintained.

The PM program could be updated to include SBOM verification and validation activities on a recurrent basis. As identified in Section 3.1.10, since using an in-house tool to generate (or verify) SBOMs may only be possible when the asset is offline, the PM schedule may depend on outages or other offline work activities. Due to the large number of digital assets in an NPP, the project team should perform a cost-benefit analysis to determine if this review process is worth the effort. As technology and tools improve, there may be an automatic or semi-automatic tool that can be used when systems are offline to automatically scan and generate SBOMs on larger network segments, thereby improving efficiencies. As an NPP moves towards automated or semi-automated collection of SBOM data, they will recognize improvements in efficiency and accuracy.

If not already completed, the project team should ensure that procurement, engineering change, configuration management, and asset management procedures are updated to include SBOM requirements. Whenever a digital asset is modified or a new digital asset is purchased, an SBOM should be generated (or updated) for each digital asset as part of the SBOM program. If software on a digital asset is modified or developed internally, an in-house SBOM generation tool should be used to capture

the SBOM. If the software is updated or purchased externally, the NPP should acquire the SBOM from the supplier. If the supplier cannot provide an SBOM, the NPP should use their in-house tool to generate one. The NPP may also want to use their in-house tool to validate the accuracy and completeness of an SBOM from a supplier, if possible.

In addition to procurement procedures, the SBOM program can also be integrated with C-SCRM programs. The NPP gains not only a detailed list of software components with an SBOM, but also the pedigree and provenance of the components. Understanding the pedigree and provenance provides the NPP with insights into the entire complex supply chain for the product. They can also use the SBOM data to verify integrity and authenticity using component hashes or other cryptographic tools. This complete set of data can be analyzed by the NPP to help determine the authenticity and integrity of the software in a digital asset. Understanding this information can enable the NPP to make risk-informed supply chain decisions.

3.3.2 Develop capabilities to dynamically monitor SBOM vulnerabilities

A major advantage of an SBOM program is that it allows vulnerability management activities to be completed efficiently and effectively. It is impossible to fix a software vulnerability the NPP doesn't know exists. As illustrated in Figure 2, vulnerability data and vendor vulnerability attestation reports can be integrated with SBOMs to enable the use of risk management processes to mitigate software vulnerabilities as they arise. With integrated SBOM vulnerability data, an NPP can identify known vulnerabilities, determine the impact to the NPP, and apply the appropriate mitigation, if needed.

As SBOM data acquisition becomes more automated, tools that rely on SBOM data can be enhanced and automated to perform their tasks with greater speed and accuracy. The vulnerability management process can be enhanced by integrating vulnerability data sources and vendor vulnerability attestation reports. Automation or semi-automation can eliminate manual integration of these processes to streamline the vulnerability management process using fewer overall resources. As new software vulnerabilities are discovered and vendors provide vulnerability attestation reports, automated lookups can be developed to search the SBOM repository to identify if the vulnerable software version is installed in the NPP. If the software is found in the SBOM tool, an automatic alert can be sent to plant personnel so mitigating actions can be taken if necessary.

Automation or semi-automation is achievable by integrating SBOMs with any dependent program (e.g., vulnerability information, vendor vulnerability attestation reports) using the standard machine-readable format. As vulnerability information is refreshed, queries linking unique identifiers (i.e., specific product versions) between systems can identify any new vulnerabilities in the SBOM repository.

Similar to security requirements for the repository, any communication channels used to acquire vulnerability information must be secured. The site's security requirements may preclude the use of certain monitoring solutions.

3.3.3 Establish/enhance a secured, central repository for all data

The security of the SBOM ecosystem is highly important. While collecting software information into a single repository is helpful to an NPP, it is also helpful to the adversary as SBOMs contain sensitive information about the design and operation of the NPP. And, although it is likely that sophisticated adversaries targeting an NPP already know about some software components installed in the plant, they likely do not have a complete listing. Additionally, this information is likely considered SRI (or possibly safeguards) and must be protected in accordance with the NPP's physical security and cybersecurity programs. Any information that is classified as safeguards information cannot be intermixed with SRI data unless the entire repository is protected to the level necessary for safeguards information.

Availability and distribution of this information should be limited to roles that have a "need to know" to perform their jobs. Appropriate access control, authentication, configuration management, system integrity, and incident response security controls should be applied to the system to ensure remains secure.

The access control principles of least privilege and separation of duties should be practiced for SBOM administrators and other systems that use SBOM data. Administrative access should only be granted to individuals with roles requiring administrative levels of access. Multi-factor authentication in alignment with the NPPs cybersecurity program is recommended for access to the SBOM system. NPP malware detection and response capabilities should be utilized on the SBOM system and synchronized with incident response capabilities to ensure the cybersecurity operations center is notified of any malicious activities as soon as possible. Auditing and chain of custody, including access and versioning logs, should be in place. It is also important to ensure any security requirements specified in procurement or contract agreements are in place and enforced.

3.3.4 Complete SBOM generation for all installed digital assets

Since the number of installed digital assets in an NPP is extensive, completing the SBOM generation in its entirety may take a long time, especially if the project is managed to minimize the use of resources outside of normal operational and maintenance expenses. Once the SBOM program is deployed and operational, the project team should follow the SBOM generation schedule identified in Section 3.1.10 to complete the data acquisition process. The project team should keep track of the SBOM generation process for each digital asset and modify the priority and SBOM generation schedule as needed.

Culmination of the SBOM project should result in a complete SBOM repository identifying all software installed on digital assets in the NPP OT environment. The integration of the SBOM repository with the equipment database in the asset management system will also provide further "where-found" information. This digital asset information can be cross-referenced and provided to the cybersecurity specialist or system engineer.

Once the project is completed, the team should transition all processes to normal operating procedures. Engineering and procurement procedures should prescribe the requirement for an SBOM with all new purchases or custom development. Procedures should also require an SBOM update with all modifications or software updates that impact the validity of the SBOM data. Procedures for integrated vulnerability management and other integrated process should also be transitioned to normal operation.

3.3.5 Maintain awareness of ongoing industry advancements

While SBOMs have existed for a long time, the standard SBOM formats, data elements, and majority of tools were developed in the last several years. NPPs should maintain awareness of industry progress, especially since U.S. government requirements may change, research and development is ongoing, and SBOM ecosystem tools is still an emergent market. They should seek enhancements for their existing SBOM tools as well as identify when new integration tools become available to enhance the breadth of capabilities for their data.

In addition to the NTIA, there are many industry collaborations in progress to expand the use of SBOMs. As also identified in Section 2.3, collaborations that NPPs should watch include:

- DOE-CESER SBOM Proof of Concept for the energy community [28]—joint collaboration with OT equipment vendors to develop tools and technologies for SBOM adoption into the energy sector.
- DHS-CISA ICT SCRM Task Force [27]—joint collaboration between government and industry that is working towards releasing new SBOM materials to enhance ICT supply chain resilience.

- DHS-CISA SBOM Workstreams [26]—community focused on four SBOM workstreams, (1) cloud and online applications, (2) on-ramps and adoption, (3) sharing and exchanging, and (4) tooling and implementation.
- Industrial Internet of Things Software Bill of Materials (IIoTSBOM) initiative [34]—joint collaboration between three nonprofit organizations from the European Union dedicated to improving cybersecurity for devices. They include relevant information about SBOM development, tools, and vendor capabilities.

4. NEW REACTOR BUILD

While this report was primarily written to provide guidance to existing NPPs on how to implement an SBOM program in their plant, the guidance still applies to new NPPs, with a few caveats:

- If the reader is the new NPP owner, they should require the reactor vendor to supply complete SBOMs for all digital assets in the new reactor.
- Alternatively, if reader is the reactor vendor, they should use a similar process as described in this report to require SBOMs from their suppliers for all digital assets.

In alignment with Cyber-Informed Engineering principles used during design of reactor control systems [31], it is easier to acquire SBOMs and develop a complete listing of all installed software components in the new reactor during the initial stages of the systems engineering lifecycle. The NPP owner and/or reactor vendor should require SBOMs with every procurement or contract agreement and should include procedures for generating SBOMs for in-house developed digital assets. Engineering change and configuration management procedures should require that any modifications to digital assets (including make/model/version) are captured and the SBOM is updated accordingly.

As the new NPP is constructed, both the NPP owner and reactor vendor should ensure that generated SBOMs are complete and accurate. It is recommended that the reactor vendor develop their own vulnerability integrated SBOM system so that they remain aware of all software vulnerabilities while the reactor is designed and constructed in order to mitigate vulnerabilities prior to turnover to the NPP owner. Additionally, the NPP owner should establish an SBOM program along with their other plant programs. Developing and integrating the SBOM program during construction and commissioning will provide the NPP owner with advance capabilities in vulnerability and risk management, which ultimately provides a greatly enhanced security posture.

5. CONCLUSION

Any new program suggested for the U.S. nuclear fleet must enable NPPs to remain economically viable. This report provides guidance on implementing and integrating an SBOM program into an NPPs existing programs and procedures in a “crawl, walk, run” method to minimize implementation costs while providing enhanced asset and vulnerability management benefits to the plant.

The current cyber threat environment is constantly changing, and it is anticipated that software and supply chain cyber-attacks will continue to evolve. As the critical infrastructure industry discovered with the Log4j attacks, it is paramount for an NPP to understand not only the higher-level software installed in their plant, but also the lower tier components and dependencies. The capability to rapidly identify whether a newly discovered vulnerability is present in a CDA enables plant personnel to respond and mitigate the exposure more quickly. Implementing an SBOM program and integrating it with

vulnerability information provides a quick and efficient method for identifying known vulnerabilities within the NPP while additional linkage with vendor vulnerability attestation reports provides added capabilities for risk management—including risk prioritization and mitigation—to enable the most cost-effective cyber risk decisions.

SBOMs can also be integrated with other plant programs and workflows to improve capabilities and efficiencies. SBOMs can be integrated with asset management, configuration management, and engineering change processes. And, in addition to cyber vulnerability mitigation, SBOMs can improve C-SCRM processes to enable better identification of compromises in the supply chain through evaluation of the pedigree, provenance, and integrity of SBOM characteristics.

A primary goal of this report is to provide a stepwise approach to implementing an SBOM program at an NPP slowly over time, using existing plant resources. However, this guide can be tailored to meet the requirements of the NPP, and the program can be implemented as slowly or quickly as desired. The most important step, however, is to simply start.

6. REFERENCES

[1] Diemer, H., *Factory Organization and Administration, 1st Edition*. New York, NY: McGraw Hill Book Company, Inc, 1910.

[2] *Apache Log4j Vulnerability Guidance*. Cybersecurity and Infrastructure Security Agency (CISA), Accessed on: June 2022. Available: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

[3] NTIA Multistakeholder Process on Software Component Transparency Framing Working Group, "Framing software component transparency: Establishing a common Software Bill of Materials (SBOM) 2nd Edition," 2021, Available: https://ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf.

[4] "Executive Order 14028 on Improving the Nation's Cybersecurity," Executive Office of the President, 2021, Available: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[5] U.S. Department of Commerce, "The minimum elements for a Software Bill of Materials (SBOM) pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity," 2021, Available: https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.

[6] NTIA, "How-to guide for SBOM generation," NTIA Software Transparency Healthcare POC, Available: https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf.

[7] NTIA, "Roles and benefits for SBOM across the supply chain," NTIA Multistakeholder Process on Software Component Transparency, 2019, Available: https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf.

[8] Springett, S. *OWASP Component Analysis*. Open Web Application Security Project, Accessed on: May 18, 2022. Available: https://owasp.org/www-community/Component_Analysis

[9] *Welcome to Transparency in Cybersecurity*. Transparency in Cyber, Accessed on: August, 2022. Available: https://transparencyincyber.org/

[10] *SBOMs: Securing the Software Supply Chain*. eSecurity Planet, Accessed on: August, 2022. Available: https://www.esecurityplanet.com/compliance/sbom/

[11] *CycloneDX Specification Overview*. CycloneDX Core Working Group, Accessed on: June 2022. Available: https://cyclonedx.org/specification/overview/

[12] *SPDX Specifications*. Linux Foundation, Accessed on: June 2022. Available: https://spdx.dev/specifications/

[13] ISO/IEC, "ISO/IEC 19770-2:2015 Information Technology-IT asset management-Part 2: Software identification tag," International Organization for Standardization/International Electrotechnical Commission, 2015, Available: https://www.iso.org/standard/65666.html.
[14] *Learn SBOM*. Learn SBOM, Accessed on: September 2022. Available: https://learnsbom.com/pages/home.html
[15] *SPDX Open Source Tools*. The Linux Foundation, Accessed on: September 2022. Available: https://spdx.dev/tools-community/
[16] *SPDX Commercial (Proprietary) Tools*. The Linux Foundation, Accessed on: September 2022. Available: https://spdx.dev/tools-commercial/
[17] *CycloneDX Tool Center*. Accessed on: September 2022. Available: https://cyclonedx.org/tool-center/
[18] *Software Identification (SWID) Tools*. NIST, Accessed on: September 2022. Available: https://pages.nist.gov/swid-tools/
[19] *Common Vulnerabilities and Exposures (CVE)*. The MITRE Corporation, Accessed on: September 29, 2020. Available: https://cve.mitre.org/
[20] *National Vulnerability Database (NVD)*. National Institute of Standards and Technology, Accessed on: September 29,, 2020. Available: https://nvd.nist.gov/
[21] CISA, "Vulnerability Exploitability eXchange (VEX) -- Use cases," VEX Working Group, Cybersecurity and Infrastructure Security Agency, 2022, Available: https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_April2022.pdf.
[22] NIST. *Executive Order 14028, Improving the nation's cybersecurity, Software security in supply chains: Software Bill of Materials (SBOM)*. Accessed on: June 2022. Available: https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1
[23] Boyens, J., A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, "NIST Special Publication 800-161r1 Cybersecurity supply chain risk management practices for systems and organizations," 2022.
[24] Souppaya, M., K. Scarfone, and D. Dodson, "NIST SP 800-218: Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," National Institute of Standards and Technology, 2022, Available: https://csrc.nist.gov/publications/detail/sp/800-218/final.
[25] NTIA. *National Telecommunications and Information Administration Software Bill of Materials*. Accessed on: June 2022. Available: https://ntia.gov/SBOM
[26] *Software Bill of Materials*. CISA, Accessed on: September 2022. Available: https://www.cisa.gov/sbom
[27] CISA. *Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force*. Cybersecurity and Infrastructure Security Agency, Accessed on: June 2022. Available: https://www.cisa.gov/ict-scrm-task-force
[28] INL. *Idaho National Laboratory Software Bill of Materials: Exploring a proof of concept for the energy community*. Accessed on: June 2022. Available: https://inl.gov/sbom-poc/
[29] OASIS, "Common Security Advisory Framework 2.0," 2021, Available: https://docs.oasis-open.org/csaf/csaf/v2.0/cs01/csaf-v2.0-cs01.zip.
[30] *The U.S. Department of Energy (DOE) National Cyber-Informed Engineering (CIE) Strategy Document*. U.S. Department of Energy, Accessed on: September 2022. Available: https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document
[31] Eggers, S. and R. Anderson, "Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control," in *Nuclear Reactors*, Chad Pope, Ed. London, UK: IntechOpen, 2022.
[32] EPRI, "Digital engineering guide: Decision making using systems engineering," Electric Power Research Institute, 2021.

[33] EPRI, "Cyber security technical assessment methodology, risk Informed exploit sequence identification and mitigation, Revision 1," Electric Power Research Institute, 2018.
[34] *Security and Software Bill of Materials for IoT*. IIoTSBOM, Accessed on: August, 2022. Available: https://www.iiotsbom.com/