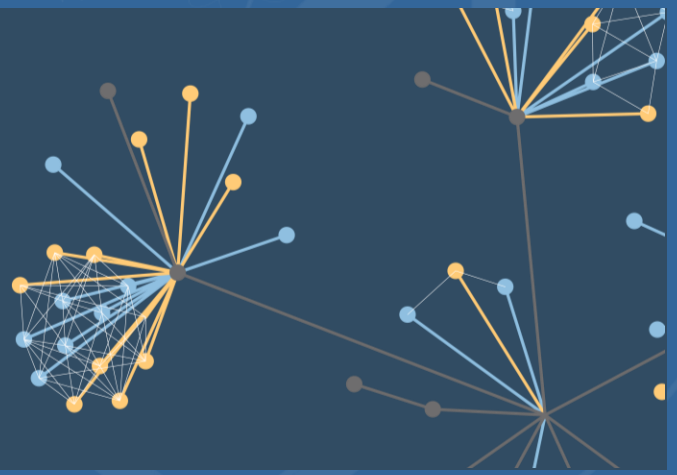
U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response

DOE CESER Energy Sector **BOM Collaboration Webinar**

NOVEMBER 18, 2024 | 12PM - 2PM EST



Agenda

Speaker	Topic
Stephanie Johnson, Ph.D., U.S. Department of Energy (DOE)	Introduction to DOE CESER's Energy SBOM POC and SBOM working group
Allan Friedman, Ph.D., Cybersecurity and Infrastructure Security Agency (CISA)	Overview of CISA efforts
Steve Kunsman, Hitachi Energy	International Standards
Gabe Weaver, Idaho National Laboratory (INL)	EO14017 - Securing America's Supply Chain Update
Animesh Pattanayak, Pacific Northwest National Laboratory (PNNL)	ESIB BOM Landscape Overview

Agenda

Speaker	Topic
Host: Aaron Wegner, Lawrence Livermore National Laboratory (LLNL) ***Panelist:*** Cassie Crossley, Schneider Electric ***Panelist:*** Stephen Trachian, Hitachi Energy	Panel 1: Vendor Perspectives on BOM Use & State of the Art
Host: Gabriel Weaver, Idaho National Laboratory (INL) ***Panelist:*** Alex Waitkus, Southern Company ***Panelist:*** Blake Gilson, ExxonMobil ***Panelist:*** Becky Burden, Snohomish County Public Utility District ***Panelist:*** Kevin Johnston, Snohomish County Public Utility District	Panel 2: Asset Owner Operator Perspectives on BOM Use & State of the Art
Jessica Smith, Pacific Northwest National Laboratory (PNNL)	Closing Remarks

Welcome

- Stephanie H. Johnson, Ph.D.
  Program Manager, U.S. Department of Energy (DOE)

CESER's Software Bill of Materials Work

- CyTRICS - System component enumeration
  - Developing tools & techniques for BOM generation, validation, and comparison
  - Work with CyTRICS partners on BOMs & keeping an eye on market solutions

- BOMs could be an enabling technology for supply chain risk management…
- *But not yet*

- We've identified several problems that prohibit SBOM usage @ scale
  - BOMS vary from one vendor to the next
  - How to verify completeness, accuracy, and trustworthiness
  - Who's responsible for vulnerabilities indicated by SBOMs?
  - … and many more

- We're actively planning research to solve these problems
  - Have specific problems you want DOE to be aware of, or want to be a part of finding solutions?
  - Contact robert.erbes@inl.gov and lucas.tate@pnnl.gov

Overview of CISA BOM Efforts

- Allan Friedman, Ph.D.
  Senior Advisor and Strategist, Cybersecurity and Infrastructure Security Agency (CISA)

SBOM International Standards

- Steven Kunsman
  VP Business Development and Marketing Grid Automation North America,
  Hitachi Energy

PUBLIC

HITACHI
Inspire the Next

Energy Sector SBOM Collaboration Webinar International Standards (and Regulations)

November 18, 2024

Hitachi Energy

Steven Kunsman steven.a.kunsman@hitachienergy.com

Director of Product Management and Applications - Grid Automation, North America

Hitachi Energy

Steve joined Hitachi Energy (formerly ABB) in 1984 and has over 40 years of experience in substation automation, protection and control. He is a graduate of Lafayette College with a BS in electrical engineering and Lehigh University with an MBA concentrated in management of technology. Steve holds 5 patents in the protection and control application area.

Industry Involvement:

- IEEE PES Power System Communications and Cybersecurity (PSCC) committee
  - Past PSCCC Cybersecurity Subcommittee chairperson
- IEEE PES Power System Relaying and Control (PSRC) committee
  - Past working group chair for substation cyber security and relay quality processes
- Participated in US Department of Energy‘s Securing Energy Infrastructure Exective Task Force
  - Senior Technical Advisor and Co-chair Evaluating Technology and Standards Technical Project Team
- ISA99 Industrial Automation and Control Systems Security Standards Committee
  - Working Group 5 member
  - Co-chair of Working Group 14 developing Electric Energy OT Control System Reference Architecture and Application Profiles mapping to IEC 62443 standards

IEEE PES PSCCC SBOM Task Force - Scope

HITACHI
Inspire the Next

Technical Committee on Power System Communications and Cybersecurity (PSCCC)

Industry Technical Standards, Guides, and Best Practices

Providing scientific and engineering information on electric power and energy for the betterment of society.

PSCCC S17: ***Task Force on Use of SBOM in the Energy Sector***

Chair: Eric Thibodeau **Vice-Chair**: Steve Kunsman

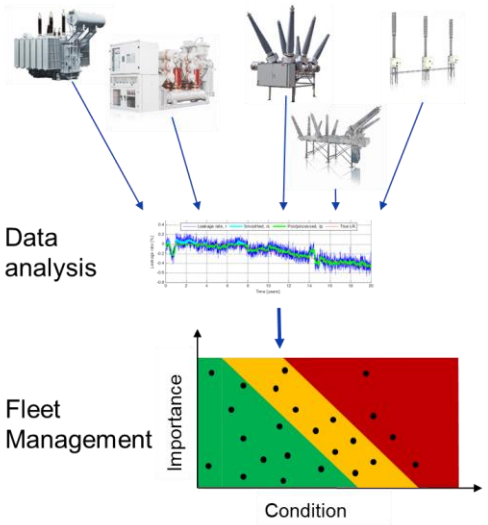
Developing a report to summarize the current efforts by external entities for the use of SBOM in Electric Power System (EPS). The task force will attempt to identify gaps in current industry efforts in order to provide guidance for future work to the Cybersecurity subcommittee.

Focus area on Asset Owner SBOM use cases and their value

Hitachi Energy

IEEE PES PSCCC SBOM Task Force - Asset Owner Utilization of SBOM/HBOM

HITACHI
Inspire the Next



SBOMs and HBOMs Utilization:

- Support the Asset Owner's purchase and lifecycle management of cyber assets or software system
  - Provide visibility into the software components prior to asset or software purchase
  - Aid in identifying currently known vulnerabilities which might exist in the cyber asset at time of purchase
  - Support system lifecycle and vulnerability management/mitigation for future discovered vulnerabilities
  - From a cybersecurity perspective, the HBOM should focus on the active components especially those involved in the software / firmware execution versus passive components

A few challenges being identified:

- Adoption from the vendor community over concerns arise from SBOM and HBOM publication
  - Includes intellectual property disclosure
  - Provides adversaries with insight on potential vulnerability exploitations before availability of mitigations or a remediation patch
- SBOM adoption is in its infancy with the various industry efforts from DHS/CISA and DOE
- SBOM assessment will identify potential vulnerabilities but by itself is not enough!
  - Vendor collaboration is important as the identified SBOM vulnerability might not be exploitable
  - A deeper understanding of the software architecture is required to avoid unnecessary cyber asset mitigation or remediation.
  - Similarly, HBOMs may identify chips/active components that have potential vulnerabilities but require an assessment if these vulnerabilities are exploitable.

Hitachi Energy

ISA99/IEC TC65 – ISA/IEC 62443

HITACHI
Inspire the Next

International Society of Automation

International Electrotechnical Commission

ISA/IEC 62443 series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS).

There are requirements throughout the 62443 for cyber asset inventories, but no specific requirements for SBOM or HBOM

Any future work would be in the scope of the JT-62443-4-1 team because it would be the Product Suppliers that would need to generate the SBOM

US National Cybersecurity Strategy – Shift of Liability

Strategic Objective 3.3: Shift Liability for Insecure Software Products and Services

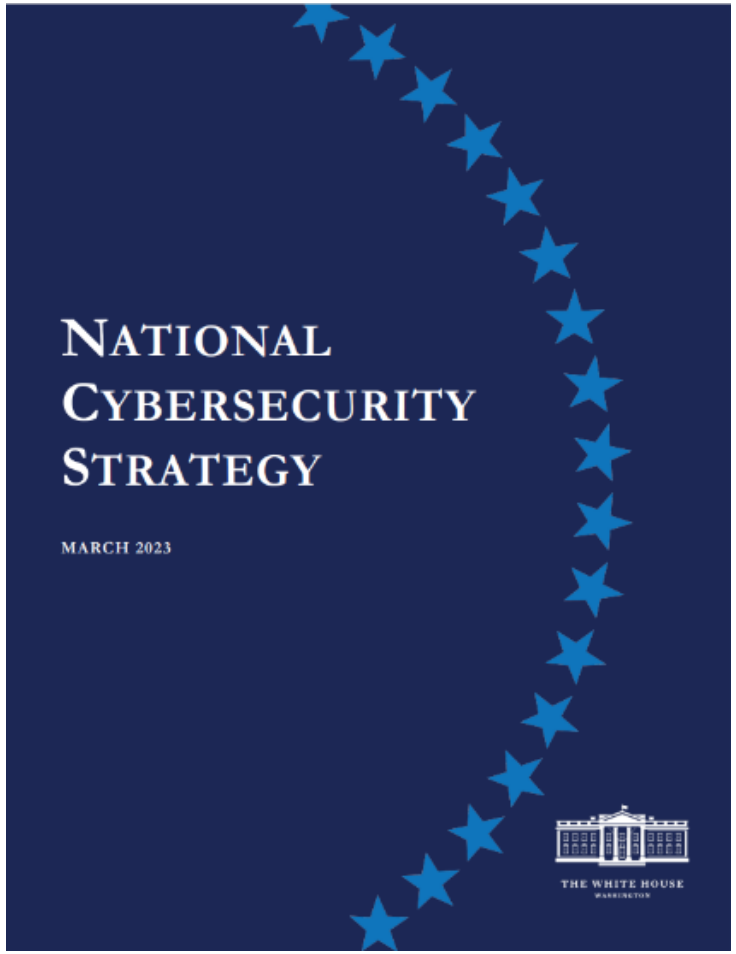
Markets impose inadequate costs on—and often reward—those entities that introduce vulnerable products or services into our digital ecosystem. Too many vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown provenance. Software makers are able to leverage their market position to fully disclaim liability by contract, further reducing their incentive to follow secure-by-design principles or perform
increases systemic risk across the digital ecosyst
cost.

We must begin to shift liability onto those entiti
their software while recognizing that even the n

prevent all vulnerabilities. Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers. Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software nor on the open-source developer of a component that is integrated into a commercial product. Doing so will drive the market to produce safer products and services while preserving innovation and the ability of startups and other small- and medium-sized businesses to compete against market leaders.

The Administration will work with Congress and the private sector to develop legislation establishing liability for software products and services. Any such legislation should prevent manufacturers and software publishers with market power from fully disclaiming liability by contract, and establish higher standards of care for software in specific high-risk scenarios. To begin to shape standards of care for secure software development, the Administration will drive the development of an adaptable safe harbor framework to shield from liability companies that securely develop and maintain their software products and services. This safe harbor will draw from current best practices for secure software development, such as the NIST Secure Software Development Framework. It also must evolve over time, incorporating new tools for secure software development, software transparency, and vulnerability discovery.

To further incentivize the adoption of secure software development practices, the Administration will encourage coordinated vulnerability disclosure across all technology types and sectors; promote the further development of SBOMs; and develop a process for identifying and mitigating the risk presented by unsupported software that is widely used or supports critical infrastructure. In partnership with the private sector and the open-source software community, the Federal Government will also continue to invest in the development of secure software, including memory-safe languages and software development techniques, frameworks, and testing tools.

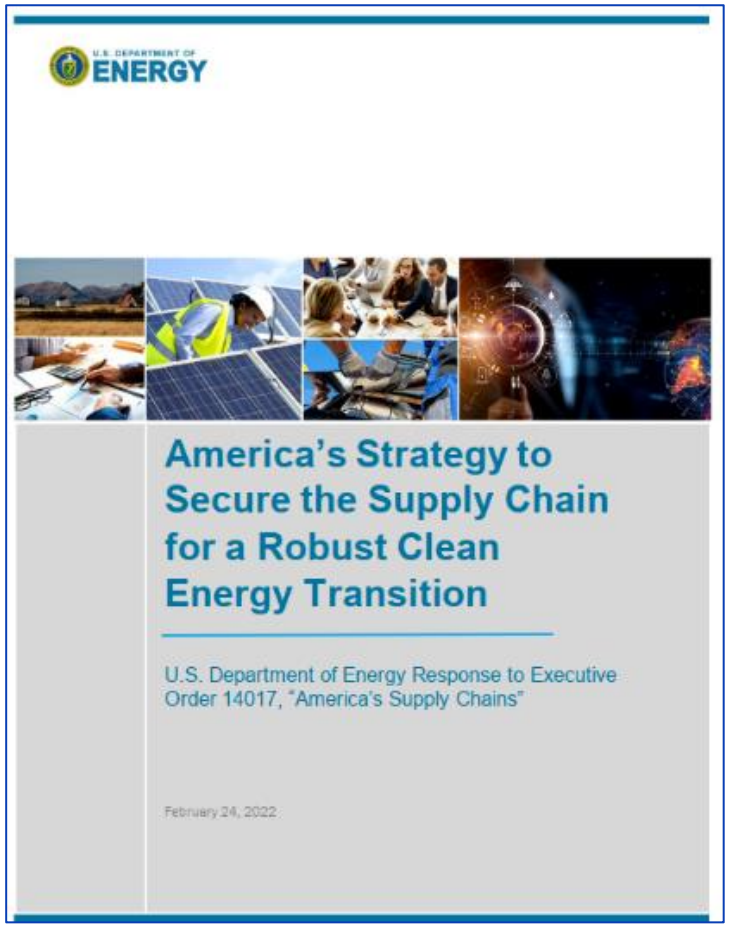


National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov)

Supply Chain Risk Management citing SBOMs

HITACHI
Inspire the Next

EO 14017 and 14028



America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition

27. Engage government and private sector to create national standards, guidelines, and requirements for the security of energy-related software, firmware, virtual platforms and services, and data. **(DOE, DOC/NIST, DHS, DOT, DOD)**

To address fragmented and inconsistent oversight of supply chain risks for digital components in critical energy systems, DOE, in consultation with other Federal agencies including DOC/NIST, DHS, DOT, and DOD, will undertake steps to develop consistent standards and guidelines to manage shared cybersecurity risks more effectively in digital supply chains for the ESIB. These efforts will leverage and build upon actions directed in Executive Order 14028, "Improving the Nation's Cybersecurity," and on efforts completed by the Securing Energy Infrastructure Executive Task Force pursuant to Fiscal Year 2020 NDAA section 5726, as well as incorporate new initiatives directed under section 40122 of the BIL, the Energy Cyber Sense Program. Specific actions will include:

- Leverage existing sources of standards and guidance within the energy sector, from other applicable sectors, and from global standards bodies to develop additional guidelines for the ESIB for critical digital supply chains that secure software, virtual platforms, datasets, and digital components. This will leverage the existing work of the Securing Energy Infrastructure Executive Task Force on evaluating the standards used to secure industrial control systems mandated under Fiscal Year 2020 NDAA section 5726.

- Identify, characterize, and assess global supply chains for critical digital components (including software, virtual platforms and services, and data) in ESIB systems, to include the bulk electric system, to inform cyber supply chain analyses. Characterization of information should include factors such as foreign provenance, ownership, control, and influence for prime and sub-tier suppliers.

- Develop guidance on the use of software and hardware bills of materials to illuminate risk in critical software supply chains and virtual platforms used in ESIB. This work will build on existing efforts underway at DOE and expanded under section 41022 of the BIL, the Energy Cyber Sense Program.

- Establish a technical R&D program to further develop capabilities to automate generation of software and hardware bills of materials for energy system components to illuminate software supply chain risks in commercial transactions at scale.

Hitachi Energy

DOE's Supply Chain Cybersecurity Principles for Suppliers

HITACHI
Inspire the Next

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Supply Chain Cybersecurity Principles

Dept of Energy released Supply Chain Cybersecurity Principles in June 2024

- A set of principles for Supplier and a set for End Users
- SBOMs will be a tool to support Transparency & Trust Building through software and hardware composition of products

Supply Chain Cybersecurity Principles for Suppliers

Impact-Driven Risk Management
Embed consideration of impacts, specifically including those in your own upstream supply chains, throughout the entire systems engineering lifecycle, seeking to manage risks to functions that are aided by digital technologies.

Framework-Informed Defenses
Incorporate appropriate principles and practices from recognized cybersecurity frameworks into the design of your organization's defenses of its critical functions, infrastructure, and information.

Cybersecurity Fundamentals
Follow relevant domain-specific regulations and international standards, and consider secure and cyber-informed engineering and design principles, to produce products and deliver services with appropriate security features and controls.

Secure Development & Implementation
Use a secure systems development lifecycle process informed by internationally accepted frameworks and standards to encourage adequate security practices throughout an offering's lifecycle.

Transparency & Trust Building
Provide appropriate information to your end users and the public regarding your cybersecurity posture, interoperability, product security, testing methods, independent verifications, and software and hardware composition of your products.

Implementation Guidance
Provide hardening and secure implementation guidance to end users, including transparent information on default settings and behaviors that must be changed or managed in implementation.

Lifecycle Support & Management
Provide appropriate product support, including security patches and mitigations, from transaction through the announced end of lifecycle support.

Proactive Vulnerability Management
Maintain a vulnerability management process—aligned to industry best practices and applicable coordinated vulnerability disclosure processes—for the responsible handling and coordinated disclosure of vulnerabilities.

Proactive Incident Response
Develop and maintain appropriate incident response plans for incidents within your own environments and when supporting end users in responding to incidents involving your products or services.

Business & Operational Resilience
Continually improve your organization's practices and offerings by identifying and implementing adaptations informed by observations, insights, and lessons learned from ongoing operations, end-user experiences, and incident response.

Supply Chain Cybersecurity Principles

Hitachi Energy

EU Cyber Resilience Act (CRA) / DE TR-03183

Cyber Resilience Act (published 15-Sept-2022) Goals:

1. Create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and
2. Create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

SBOMs in the CRA

- Manufacturers to draw up an SBOM in a commonly used format covering at the very least the top-level dependencies of the product No requirement to make the SBOM publicly available
- SBOM to be included in the technical documentation and, upon request, to be provided to market surveillance authorities
- Commission empowerment to specify the format and elements (international standards to be relied upon)

Germany Federal Office for Information Security

- Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products https://bsi.bund.de/dok/TR-03183
- Aims to provide manufacturers with advance access to the type of requirements that will be imposed on them by the future Cyber Resilience Act (CRA) of the EU
- Part 2: Software Bill of Materials (SBOM)

SBOM Requirements in the CRA (Cyber Resilience Act) - FOSSA

ISO/IEC JTC 1/SC 27 ISO/IEC 27036 - Cybersecurity — Supplier relationships

HITACHI
Inspire the Next

Standard ID	Standard title	Rationale	Gap	Life-Cycle
ISO/IEC 27036 **Parts 1 to 3**	Cybersecurity — Supplier relationships — Part 1:2021 Overview and concepts Cybersecurity — Supplier relationships — Part 2:2022 Requirements Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security	This standard covers information security for supplier relationships. It provides guidance on managing information security risks associated with suppliers and third-party developers. This can be relevant to SBOM in the context of the software supply chain.	While it is relevant to the overall supply chain, it doesn't specifically address the creation, management, or exchange of Software Bill of Materials (SBOM).	Design Surveillance Maintenance

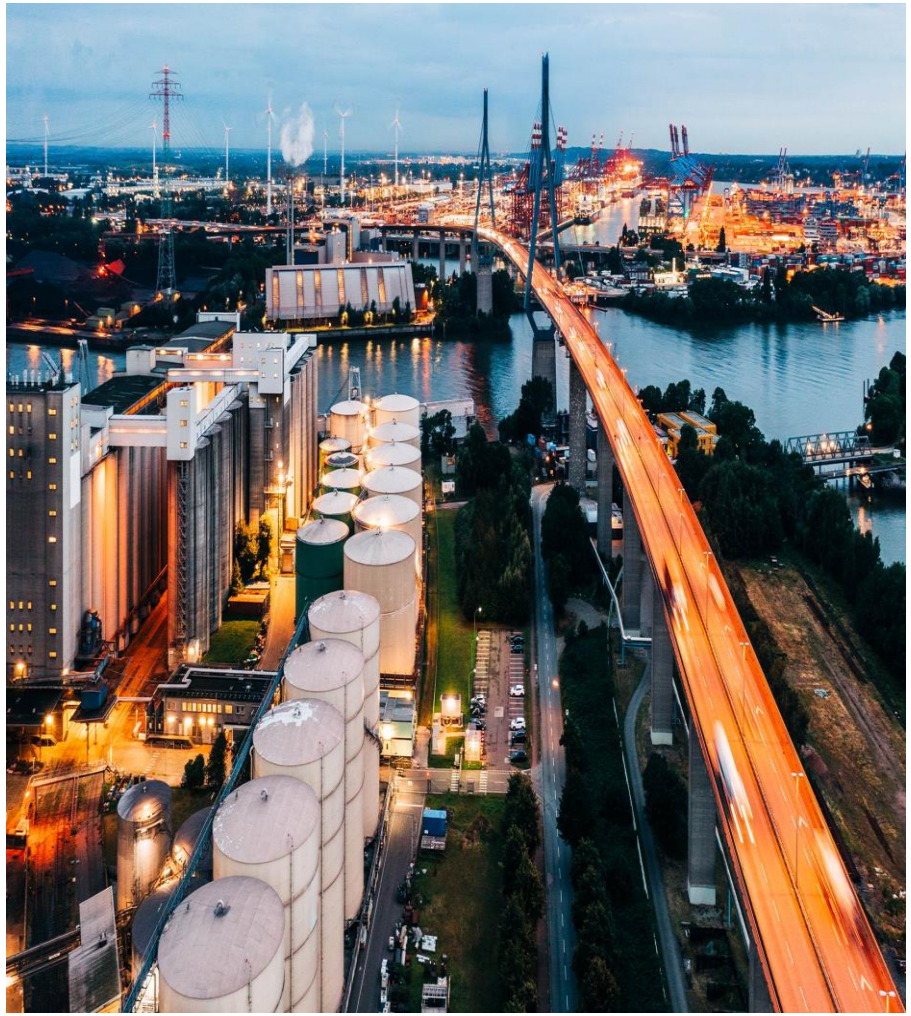
Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis — ENISA

CRA Requirements Standards Mapping by ENISA identifies ISO/IEC 27036 to provide guidance on security risks

… relevant for SBOMs

Hitachi Energy

Summary – SBOMs in Energy Sector Standards



- SBOM international standards activities slow to ramp up
  - Making CISA's SBOM effort very important
- Driving SBOM adoption and utilization
  - EU regulation and acts
  - Asset Owner inclusion in supply chain specification
- Be involved and an advocate:
  - Participation in the Energy Sector Software Bill of Materials Proof of Concept (POC) is a great community to engage
  - Support the SBOM effort led by DHS/CISA focused on moving the industry forward
    - This is an important step toward adoption
  - Join the IEEE PES PSCCC S17 SBOM task force to help define the gaps and support the development of Asset Owner use cases

HITACHI

Inspire the Next


Hitachi Energy

EO14017 - Securing America's Supply Chain

- Gabriel Weaver

  Senior Critical Infrastructure Analyst, Researcher, Idaho National Laboratory (INL)

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response

Cyber Supply Chain Risk Management (C-SCRM) in the Energy Sector

Use Cases for SBOM

Douglas Buddenbohm, Matthew Perrie, ***Gabriel A. Weaver***

LRS: INL/MIS-24-82024

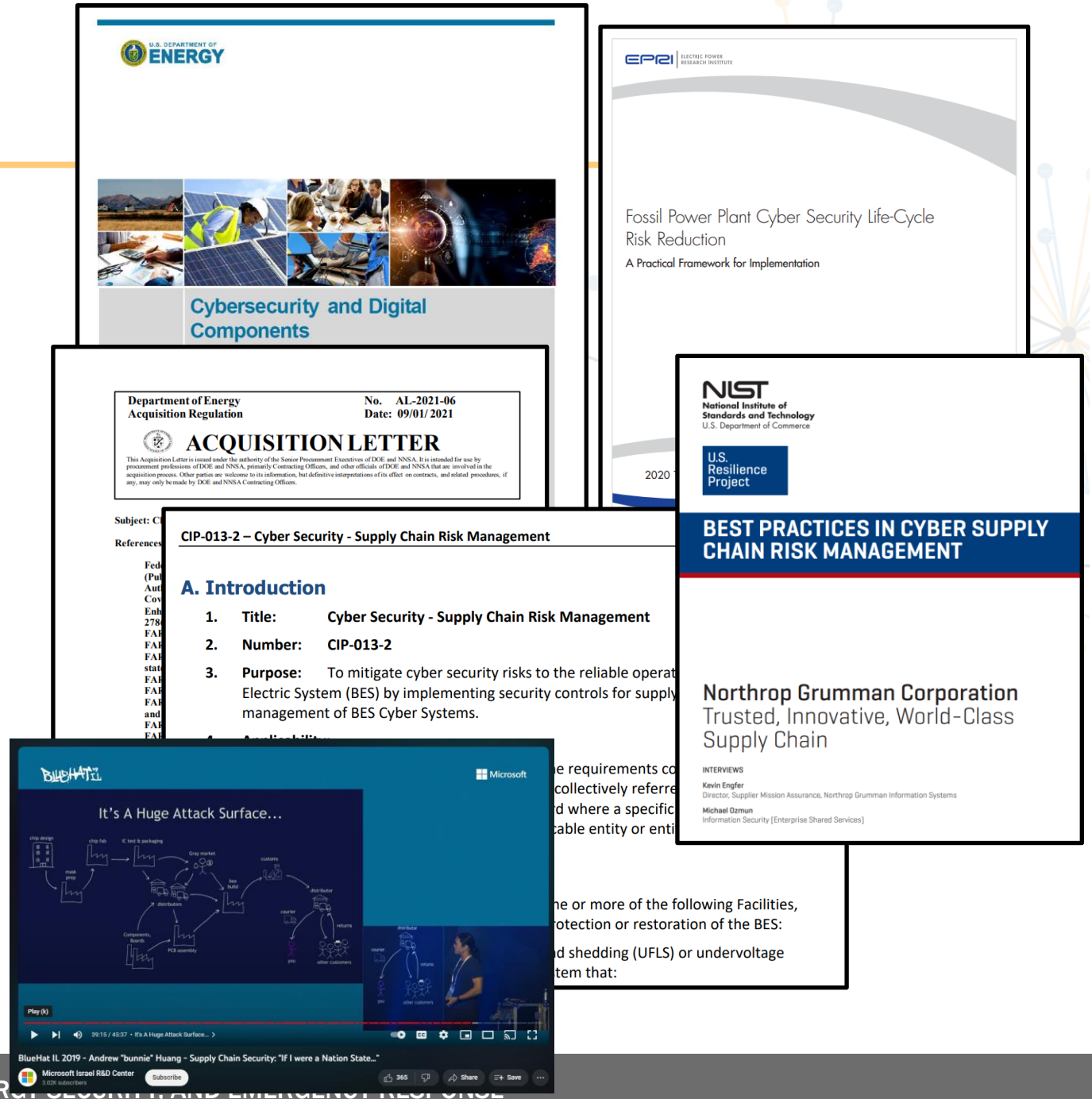
Introduction

Executive Order (EO) 14017: America's Strategy to Secure the Supply Chain for the Energy Sector.

Objective: Provide stakeholders with a practical approach to manage and mitigate unexpected impacts through the digital supply chain.

Approach: Review state of the art and state of the practice:

1. Align terminology across industry and scientific research.
2. Identify obstacles faced by stakeholders to implement C-SCRM programs.



Background

Motivation: In order to implement digital SCRM programs, stakeholders need to scope the digital supply chain problem.

We analyze historical cyber SCRM incidents:

- the type of *digital component*
- the *lifecycle stage* of the impacted digital components
- *obstacles* to prevent and respond to such events
  - Organizational
  - Procedural
  - Technological

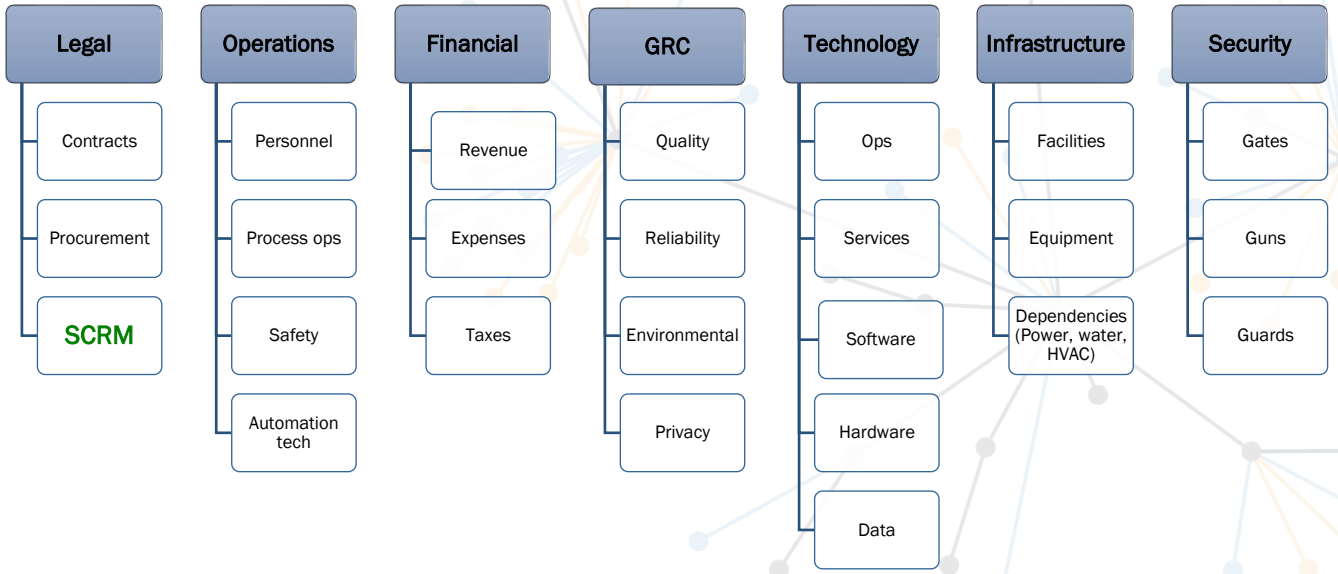
Component	Event	Date	About	Pattern
Hardware	Applied Materials[43]	2/2023	• "negative estimated impact of $250M due to a cybersecurity event recently announced by one of our suppliers".[44] • MKS Instrument Inc, a supplier for Applied Materials (assumed).	• Vendor: Impact.Loss of Availability (TO826) • Customer: Impact.Loss of Productivity and Revenue (TO828)
Firmware	PKFail	5/2012	• Produced AMI test key for firmware used for different Intel and ARM-based device makers. • Potentially millions of consumer and enterprise devices around the world that are currently using the same compromised AMI Platform Key. • The attacker can deploy Unified Extensible Firmware Interface (UEFI) bootkits, which offer persistent kernel access and privileges.	• Vendor: Exploitation for Privilege Escalation (T1068) • Customer: Impact.Loss of Productivity and Revenue (TO828)
Software	Polyfill[45]	2/2024	• Chinese company acquires company that manages polyfill library. • The OSS library handles advanced, non-native JavaScript functions on old OS browsers. • After acquisition, the library started to redirect clients to potentially-malicious sites sporadically.	• Vendor: Acquisition for Persistence. • [Customer Systems]: Impact.Manipulation of Control
Services	Okta[46]	3/2022	• The Lapsus$ Group claimed it had gained access to an administrative account for Okta.	• [Vendor Systems]: Lateral Movement.Valid Accounts (TO859) • [Vendor Systems, Customer Data]:

Relevance of SBOM to C-SCRM Workflows

- SBOM are an emerging technology with potential use cases for C-SCRM.

- Important to consider:
  - How SBOM may integrate into SCRM activities for both Vendors and Asset Owners.
  - Potential obstacles to implement those activities.

- Specifying workflows for SBOM is a research topic in and of itself (e.g. Blask et al.)



SBOM Obstacles: Asset Owner (AOO) Software Procurement

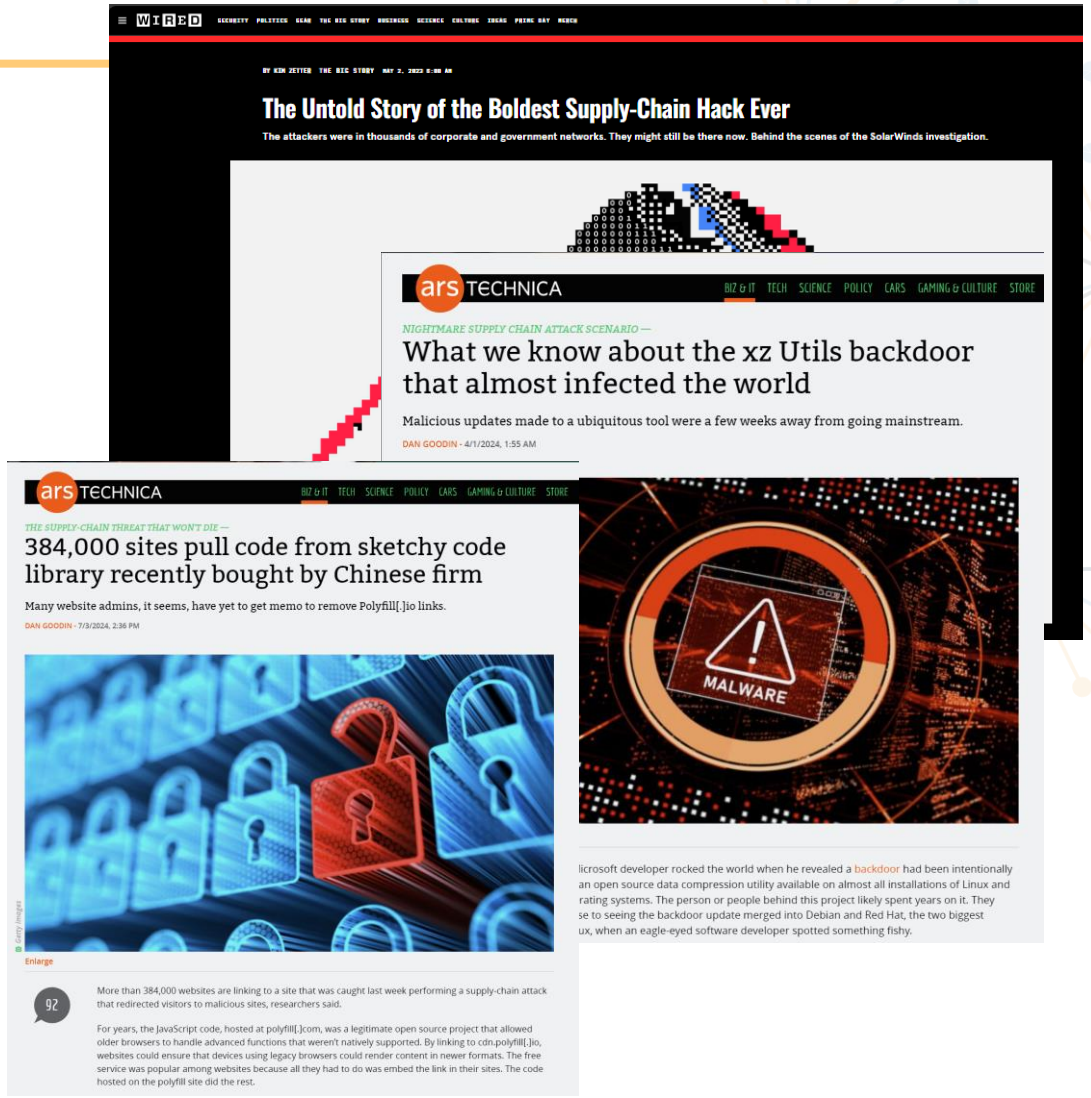
	Organizational	Technical
Availability	• Vendors may go out of business • Small businesses may not be able to provide an SBOM • CVE counts associated with a published SBOM are potential reputation risk	• Previous versions of software may not be supported • Different taxonomic types of dependencies (runtime, build, service, platform).
Data Quality	• Limited coverage of assets by vendors in the Energy Sector.	• Data integrity • How to verify and validate contents of SBOM • Translation over formats is lossy • Lack of in-depth SBOM quality metrics • No common naming conventions

SBOM Obstacles: AOO Software Operations & Maintenance

	Organizational	Technical
Generation	• SBOM unavailable from Vendor • Legal obstacles to reverse engineer to generate SBOM. • Right to repair laws a factor	• Multiple ways to create an SBOM for the same piece of software. • tools don't auto-detect everything • SBOM for Operating Systems are a different beast • SBOM capture a single point in time
Comparability	• SBOMs can allow one to interpret different fields as equivalents.	• How to compare BOM across versions? • What about product downloads/patching/configurations? (SBOM drift) • Even if the same format, BOMs not the same

Conclusion

- Our research catalogs obstacles to implementation of high-level guidance for C-SCRM programs.
- Software is just one type of component in the digital supply chain.
- SBOM *may* be useful across a number of C-SCRM workflows.
- However, SBOM also introduce their own unique challenges/obstacles.
- Please reach out to continue the conversation.



ESIB BOM Landscape Overview

- Animesh Pattanayak
  Cyber Security Engineer, Pacific Northwest National Laboratory (PNNL)

Background

- Lead development of BOM Roadmap for DOE CESER Energy Cyber Sense (ECS)
  - PI: Kathryn Walsh (LLNL)
  - Supporting: Aaron Wegner (LLNL), Animesh Pattanayak (PNNL)
- Sponsor: DOE CESER
- DOE Lab Coordination: LLNL, INL, PNNL, SNL

What is a Bill of Materials (BOM)?

- Listing of components which make up a system
- Nested inventory
- Hierarchical relationships
- SBOM and HBOM amongst others

Why BOMs?

- Supply Chain Risk Management
- Digestible
- Machine Readable
- Procurement Process
- Vulnerability Management
- Incident Response

Not All BOMs Are Created Equal

- BOM Types
- BOM Format
- BOM Schema
- BOM Quality

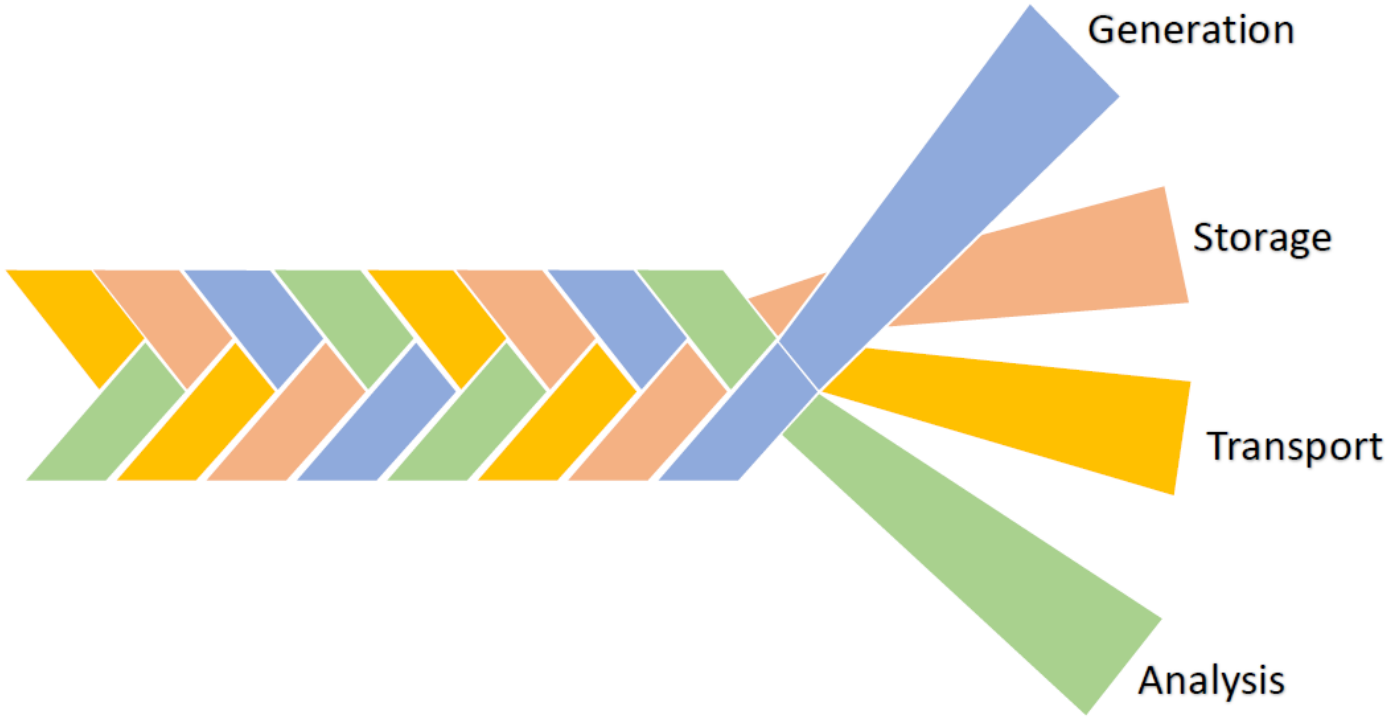
BOMs in the Energy Sector

- Primary Stakeholders
  - Government
    - EO 14028
    - NTIA, CISA, NSA, etc.
  - Vendors/Manufacturers
    - BOM variability – source vs build
    - No small feat
  - Asset Owners and Operators
    - Size variability in environment and teams
    - Resource constraints
- Challenges
  - Vendor Concerns about Intellectual Property
  - Device Lifespan
  - Legacy Technology
  - Risk of False Positives and False Negatives

The Roadmap

- EO 14028 (2021) – Call for BOM Usage
- BOM Maturity
- How do we get from A to B?

BOM Operationalization Braid



SME Engagement Emerging Themes

- Call for Common Language and Standards of Practice
- Measuring BOM Accuracy or Completeness
- Boundaries with Data Protections
- Better Understand Industry Needs

The Vendor Perspective

Panel 1

Cassie Crossley, VP Supply Chain Security, Schneider Electric

Stephen Trachian, Cybersecurity Application Engineer, Hitachi Energy

Moderator

Aaron Wegner, Software Engineer, Lawrence Livermore National Laboratory (LLNL)

The AOO Perspective

Panel 2

Alex Waitkus, Principal OT Cyber Architect, Southern Company

Blake Gilson, Industrial IT Cyber Security Operations Manager, ExxonMobil

Becky Burden, CIP Compliance Analyst, Snohomish County Public Utility District

Kevin Johnston, Senior Manager, Information Security Snohomish County Public Utility District

Moderator

Gabriel Weaver, Senior Critical Infrastructure Analyst, Researcher, Idaho National Laboratory (INL)

Closing Remarks

- Jessica Smith
  Senior Cybersecurity Research Scientist, Pacific Northwest National Laboratory (PNNL)

Thank You

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response