Supplier Sharing Call

June 19, 2024

NATF members guidelines for this call

- This is an open call
- Some participants on this call are not employees of NATF member companies
  - Do not share confidential information
  - Avoid conduct that unreasonably restrains competition
  - Adhere to your organization's standards of conduct
  - Do not share intellectual property unless authorized

Guidelines for this call

- This call is not recorded
- Slides will be available on the NATF public website at: Supplier Sharing Calls (natf.net)

NATF does not endorse specific solution providers and provides content for entity awareness of available resources.

Please participate

- Raise your hand
  - We will unmute you
  - Make sure you are identified in the participant list
- Put a question or comment in the chat
- Put a question or comment in the Q&A

If you put a question or comment in the chat or Q&A but want to remain anonymous, please open with your request

Frank Harrill

VP, Security, SEL

Opening Remarks

Frank Harrill

Vice President, Security,

Schweitzer Engineering Laboratories (SEL)

Purpose of the NATF Supplier Sharing Calls

- The intention of these calls is to
  - encourage conversation between suppliers and with the end-users of their products and services,
  - provide a forum to share forefront security concerns and how to address them, and
  - to discuss general security practices.
- These calls are applicable to suppliers of all sizes and security maturity.

Contributing Organizations

- Aspen Technology / OSI
- Hitachi Energy
- International Society of Automation (ISA)
- National Electrical Manufacturers Association (NEMA)
- Schneider Electric
- Schweitzer Engineering Laboratories (SEL)
- Siemens
- Siemens Energy
- US Chamber of Commerce
- With support from:
  - LG&E and KU Energy
  - Nebraska Public Power District
  - Southern Company

On the call today

- **Special Guest Panelist: Cassie Crossley, VP Supply Chain Security, Schneider Electric**
- Aspen Technology / OSI – Peter Escobar, VP, Research and Development
- LG&E and KU Energy – Tony Hall, Manager, CIP and Federal Regulatory Compliance
- Nebraska Public Power District - Tony Eddleman, Director of NERC Reliability Compliance
- Schneider Electric – Michael Pyle, Director of Product Cyber Security
- Schweitzer Engineering Laboratories (SEL) – Frank Harrill, VP Security
- Siemens Industry – Andy Turke, Cyber Security Officer
- Southern Company – Jennifer Couch, Manager, Transmission EMS Compliance
- US Chamber of Commerce – Heath Knakmuhs, VP and Policy Counsel

Software Bills of Materials (SBOMs)

Panel Discussions Facilitated by:

Frank Harrill

VP Security, Schweitzer Engineering Laboratories (SEL)

Jennifer Couch

Manager, Transmission EMS Compliance, Southern Company

Cassie Crossley

VP Supply Chain Security, Schneider Electric

Michael Pyle

Director of Product Cyber Security, Schneider Electric

Tony Eddleman

Director of NERC Reliability Compliance, Nebraska Public Power District (NPPD)

Discussions

- What is an SBOM?
- The problem we are trying to solve
- Security
- Logistics
- Looking forward

What is an SBOM?

Discussion Facilitator: Cassie Crossley

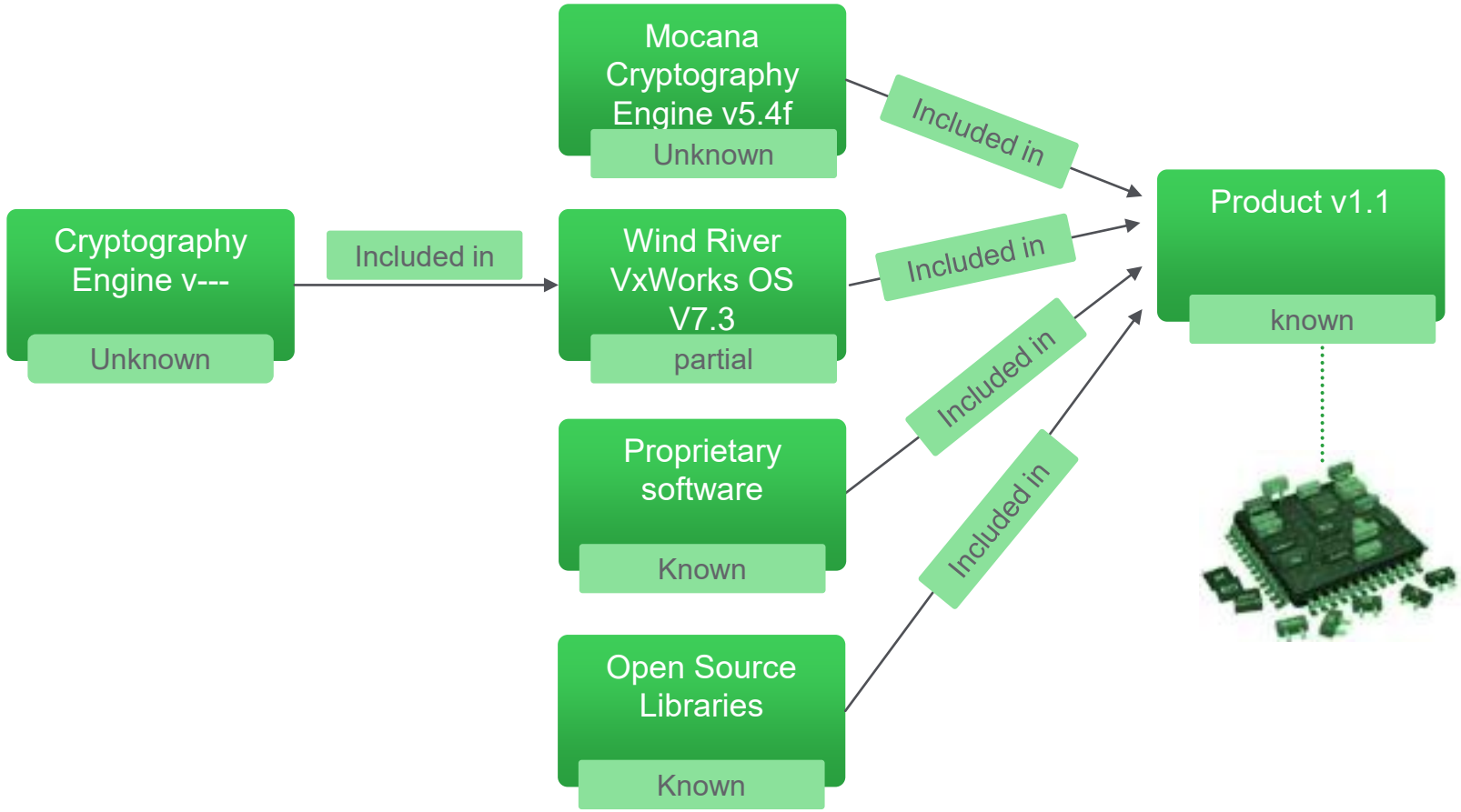
Discussion Points:

- What is an SBOM
- Requirements for SBOMs
- Maturity: SBOM Generation

What is an SBOM?

A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships for the various components used in building software.

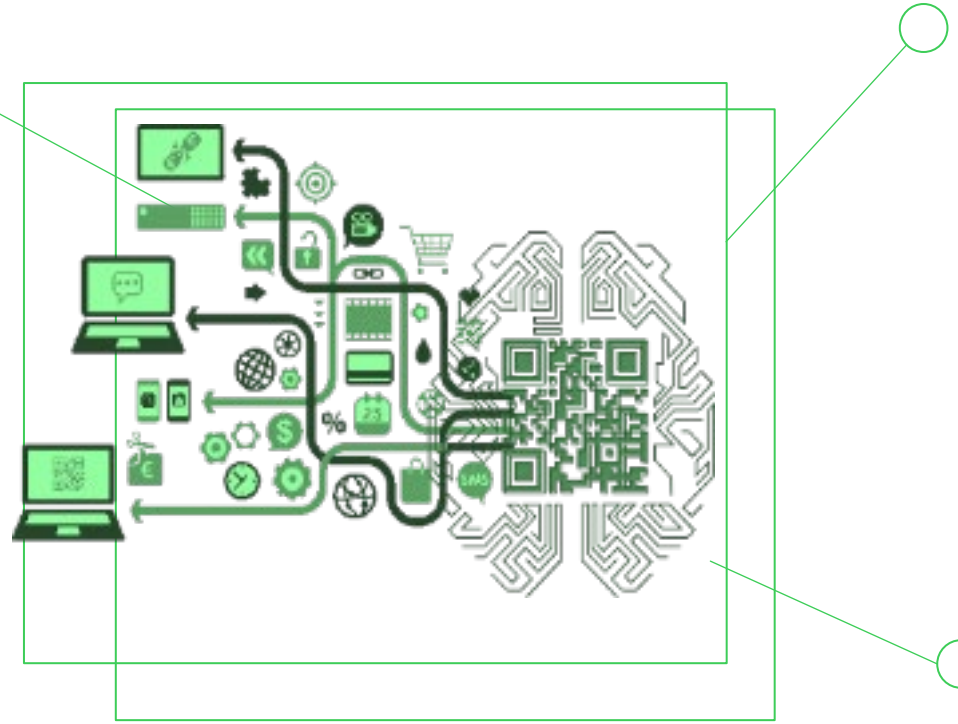
These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or access-Internal.



Requirements for SBOMs

Regulation / Compliance

- U.S. Executive Order 14028 for improving cyber security (includes a provision for SBOMs)
  - NTIA minimum requirements
  - OMB Memo M-22-18
  - OMB Memo M-23-16
- Europe Cyber Resilience Act requires SBOMs. Each EU country will release guidelines.
  - Germany - IT Security Act 2.0 and SBOM Guidelines
- Europe Digital Operational Resilience Act for Financial sector (uses the term third party components instead of SBOM)
- Australia – ISM-1730 Software Bill of Materials



US Agencies

- FDA Consolidated Appropriations Act and Patch Act 2022
- U.S. Department of Energy CyTRICS program requires the SBOMs for all products
- NIST SP 800-161 C-SCRM mentions SBOMs
- NIST SP 800-218 Secure Software Development Framework (SSDF) includes SBOMs
- CISA Secure Software Development Attestation form does not require SBOMs, but agencies are allowed to add it as a requirement

Procurement

- Required in Edison Electric Institute contract template (used by most utilities)
- NERC CIP Security Guidelines - Vendor Risk Management Lifecycle

Links

- US Department of Commerce, The Minimum Elements for a Software Bill of Materials (SBOM), July 12, 2021. (https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf)
- “Memo M-22-18: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”, Executive Office of the President, Office of Management and Budget, September 14, 2022. (https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf)
- “Memo M-23-16: Updated to M-22-18” (https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security-1.pdf)
- Germany Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products – Part 2: Software Bill of Materials (SBOM), November 28, 2023. (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2.pdf?__blob=publicationFile&v=5)
- Europe Digital Operational Resilience Act, 2022. (https://www.digital-operational-resilience-act.com/DORA_Articles.html)
- The European Parliament and Council, Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020, September 15, 2022. (https://ec.europa.eu/newsroom/dae/redirection/document/89543)

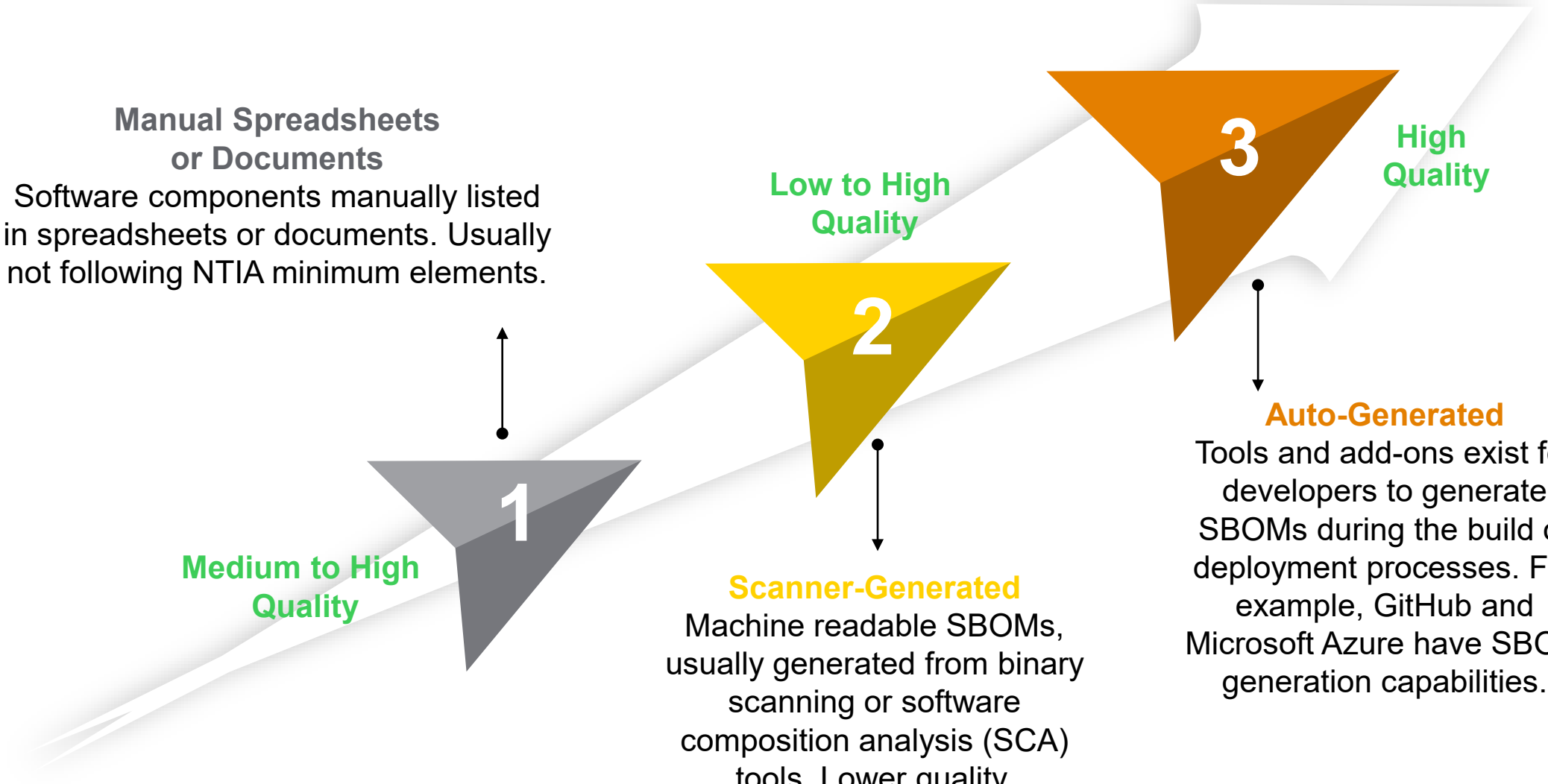
Links

- Australia – ISM-1730 Software Bill of Materials, June 13, 2024. (https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-software-development)
- US Food & Drug Administration, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions: Guidance for Industry and Food and Drug Administration Staff, September 27, 2023. (https://www.fda.gov/media/119933/download?attachment)
- U.S. Department of Energy CyTRICS program. (https://cytrics.inl.gov/cytrics/wp-content/uploads/2022/11/2022-05-04-CyTRICS-one-pg_formatted.pdf)
- NIST SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management for Systems and Organizations, National Institute of Standards and Technology, May 2022. (https://doi.org/10.6028/nist.sp.800-161r1)
- NIST SP 800-218: Secure Software Development Framework (SSDF) Version 1.1, National Institute of Standards and Technology, February 2022. (https://doi.org/10.6028/nist.sp.800-218)
- CISA Secure Software Development Attestation form, March 18, 2024. (https://www.cisa.gov/resources-tools/resources/secure-software-development-attestation-form)
- Edison Electric Institute has removed the public link to the contract template. Model--Procurement-Contract.pdf (eei.org)
- NERC CIP Security Guidelines, March 22, 2023. (https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf)

Links

- Schneider Electric presentation on how it uses SBOMs to help them with their vulnerability disclosure process: https://www.youtube.com/watch?v=TNzLRkdX2CM

Maturity: SBOM Generation



Manual Spreadsheets or Documents

Software components manually listed in spreadsheets or documents. Usually not following NTIA minimum elements.

Medium to High Quality

Low to High Quality

Scanner-Generated

Machine readable SBOMs, usually generated from binary scanning or software composition analysis (SCA) tools. Lower quality.

High Quality

Auto-Generated

Tools and add-ons exist for developers to generate SBOMs during the build or deployment processes. For example, GitHub and Microsoft Azure have SBOM generation capabilities.

The problem we are trying to solve

Discussion Facilitator: Frank Harrill

Discussion Points:

- The purpose of SBOMs
- Not a new concept
  - What's new is machine readability
  - Usefulness without a VEX – risk-based focus
- Other potential sources of inventories
- Making SBOMs usable

Security

Discussion Facilitator: Jennifer Couch

Discussion Points:

- Making the private public
- Attackers using AI
- End-users need to be able to obtain whether they are subject to a vulnerability quickly

Logistics

Discussion Lead: Tony Eddleman, Jennifer Couch

Discussion Points:

- Logistics of SBOM management
- Adapting an SBOM to an end-user's customized configuration
- An SBOM is a point in time; staying current with different versions

Looking Forward

Discussion Facilitator: Michael Pyle

Discussion Points:

- Suppliers must curate SBOMs for products
  - However, suppliers differ in ability to provide SBOMs
- 62443 and 27001 implicitly have inventories
- Approach becoming more methodical and international
  - EU Cyber Resiliency Act
- Solution providers supporting SBOMs

Additional Links provided during the call

- The White House statement: https://www.whitehouse.gov/briefing-room/statements-releases/2024/06/18/statement-from-national-security-advisor-jake-sullivan-on-the-global-effort-tostrengthen-the-cybersecurity-of-energy-supply-chains/
- The DOE press release: https://www.energy.gov/articles/doe-leads-effort-improve-cybersecurity-energy-supply-chains
- https://www.cisa.gov/sites/default/files/2024-04/Self_Attestation_Common_Form_FINAL_508c.pdf
- Software Supply Chain Security: Securing the End-to-End Lifecycle for Software, Firmware, and Hardware: https://oreillymedia.pxf.io/c/5049928/1902050/15173
- SBOMs for Evil: From Software Supply Chain Documentation to an Attack Path: https://www.youtube.com/watch?v=nB-4t31F6y4
- Myth vs. Facts: https://www.ntia.gov/files/ntia/publications/sbom_myths_vs_facts_nov2021.pdf

Questions?

Comments?

Upcoming Calls

- October 7
  - 2:00-3:00pm eastern
  - Topic to be determined

Frank Harrill

VP, Security, SEL

Closing Remarks

Frank Harrill
VP, Security Schweitzer Engineering (SEL)

Thank you for attending!

supplychain@natf.net
dearley@natf.net
vagnew@natf.net