ENERGY SECTOR SBOM POC CHARTER

PURPOSE OF THE DOCUMENT:

The Project Charter captures high level planning information (scope, deliverables, assumptions, etc.) about the SBOM Proof of Concept effort

Version 0.1
April 28, 2021

Energy Sector SBOM Proof of Concept PROJECT CHARTER

Project Name: ENERGY SECTOR SBOM[1] POC **POC Sponsors:** Allan Friedman (NTIA) Cheri Caddy (DOE)	**POC Co-leads:** Virginia Wright (INL) Tom Alrich (Consultant)
Date: 04/28/2021	**Revision Number:** .1
POC Email Address: SBOMEnergyPOC@inl.gov	**POC Website:** SBOM Proof of Concept - INL

1. PROJECT OVERVIEW

Convene a group of diverse energy-sector stakeholders in an open, transparent, consensus-based process to explore the application of Software Bills of Materials within energy sector environments, and to catalyze progress in SBOM adoption to increase transparency into software components within the sector.

In an open forum, spur the development of techniques and processes for SBOM adoption into the energy sector, including leveraging the work of the NTIA Software Transparency Initiative (SBOM) Working Groups:

- Framing Working Group – SBOM specification and structures; specification and structures of VEX (Vulnerability Exploitability Exchange) documents
- Formats & Tooling Working Group – Automation of SBOMS including tools, processes, and playbooks
- Awareness and Adoption Working Group – Outreach strategies and business cases
- Automotive Proof of Concept Working Group -- Exploring adoption of SBOM within the Automotive Sector
- Healthcare Proof of Concept Working Group -- Exploring adoption of SBOM and VEX within the Medical Device Community

[1] A Software Bill of Materials (SBOM) is effectively a list of ingredients or a nested inventory. It is “a formal record containing the details and supply chain relationships of various components used in building software" https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_energy_jan2021overview_0.pdf)

2. PROJECT GOALS

1. Gather a diverse stakeholder community incorporating technology suppliers, asset owners and third party vendors within the energy sector to share and build knowledge and experience about Software Bills of Materials (SBOMs).
2. Foster the creation and exchange of SBOM information between vendors and asset owners within the energy sector.
3. Explore use cases for leveraging SBOM's within the vendors and asset owner communities in the energy sector.
4. Identify gaps to implementation of SBOM technology and potential mitigations.[2]

3. DELIVERABLES

The SBOM Energy PoC will produce the following deliverables:

1. A series of **open workshops** during which the participants will discuss issues related to the production, distribution and use of SBOMs, including test cases and demonstrations.
2. **Production of SBOMs** by software and intelligent device suppliers to the energy industry, along with **use of produced SBOMs** by energy asset owners for supply chain risk mitigation purposes. Participation in this process will require a trusted information sharing agreement to mitigate risk in the exchange of information.
3. One or more **reports** documenting PoC activities and lessons learned.

4. SCOPE DEFINITION

The Proof of Concept will focus on multiple topics simultaneously. Additional areas of focus that may be added as the project progresses include:

1. Discussion of techniques and processes for producing SBOMs
2. Discussion of policies and legal restrictions for distribution of SBOMs
3. Discussion of methods of enhancing SBOM data for use by energy organizations
4. Discussion of use of SBOM data by existing risk management tools
5. Discussion of consumer use cases for SBOM
6. Development and dissemination of SBOMs for open source and non-sensitive products for use by working group members

The Proof of Concept will **not** include:

1. Development of new tools or technology
2. Advocacy for specific commercial tools
3. Dissemination of SBOMs provided under information sharing-agreements beyond the partners specifically identified.

[2] Gaps identified by the working group in their first meeting include legacy product challenges and the use of SBOM in regulated environments (CIP vs. non-CIP)

4. PROJECT MILESTONES

5. ASSUMPTIONS, CHALLENGES, CONSTRAINTS & DEPENDENCIES

Assumptions:

- POC stakeholders are voluntary members of the Proof of Concept exploration.
- Information provided in POC meetings and out briefs is intended as publicly available information.
- SBOM information which is intended to be protected will be exchanged under an information protection agreement.
- Initial lessons learned as a part of organizing and planning the POC will be published.
- Lessons learned through discussion in the public meetings, as well as those generated as a result of legally protected distribution of privately-generated SBOMs will be published, without specific references to SBOM suppliers, consumers, or products.
- All POC stakeholders will be provided the opportunity to perform hands-on activities with non-sensitive SBOM information, including that from open source products.
- Though a sample timeline is provided above, it is notional and will change as the POC progresses.

Challenges:

- The stakeholder team is diverse, with a variety of expertise levels in SBOM. It will be challenging to identify courses of action which equally interest and involve all parties.
- Though third party tools and services will be crucial to the success of SBOMs within the energy sector, the POC cannot advocate for the use of any specific commercial tool or service, nor can it provide a platform for advertising capabilities of specific tools or services.

Constraints:

- This POC will focus on energy sector applications for SBOM and will not address other infrastructure sectors – although many of the lessons learned will likely be applicable to other sectors.
- The POC will involve third-party vendors in protected SBOM information exchange only at the direction of POC Exchange members.
- The POC depends on a wide variety of viewpoints and thus will seek to entertain feedback from all participants, rather than limiting input to only a few.
- The SBOM POC lacks the resources to provide financial support for the activities of POC Exchange members.

Dependencies:

- Though the POC is dependent on POC Exchange Members to assemble and share information, it is not dependent on any specific entities to agree to an exchange.
- The POC will build upon the SBOM formats and ontologies developed by the NTIA Software Transparency Initiative (see below).

6. CURRENT BARRIERS TO ADOPTION

- Information release - Some producers are nervous about provided information being misused
- It's a chicken-and-egg problem – Until producers and suppliers are readily producing and consuming SBOM information, specific use cases and technical barriers are hard to discern. This is the main reason for undertaking a PoC.
- While tools for producing SBOMs are already well developed, tools for consuming SBOMs – for such purposes as vulnerability management and license management – are much less developed. One goal of this PoC is to foster development of tools for consumption.
- Diverse viewpoints and interests need to be reconciled in order to arrive at workable procedures for producing, distributing and utilizing SBOMs. Not all parties will be satisfied.

6. RELATED DOCUMENTS

- *SBOM Documents Quick Links:*
  - SBOM at a Glance
  - FAQ document
  - SBOM Options and Decision Points
  - Sharing and Exchanging SBOMs
  - Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)
  - Roles and Benefits for SBOM Across the Supply Chain
  - Survey of Existing SBOM Formats and Standards

These and other documents are available at https://www.ntia.doc.gov/SBOM. The four NTIA working groups are continually discussing and producing new documents. To participate in those weekly sessions, and/or to be included in the mailing lists for the email discussions, go to the main Software Component Transparency Initiative web page: https://www.ntia.doc.gov/SoftwareTransparency.

Executive Order on Improving the Nation's Cybersecurity

7. PROJECT ORGANIZATIONAL STRUCTURE

- **POC Stakeholders** attend POC working sessions and out brief sessions to help the proof of concept activity achieve its goals
- **POC Exchange Members** are POC stakeholders who have entered into an information sharing agreement for the purpose of protecting information exchange
- **POC Co-leads** facilitate meetings and information exchange for the POC
- **POC Sponsors**, currently NTIA and DOE, provide resources and staff to aid the POC achieve its goals.