Mission Statement

Develop and execute an approach for how manufacturers and vendors can communicate useful and actionable information about the third-party/embedded software components that comprise modern software and IoT devices, and how this data can be used by enterprises to foster better security decisions and practices.

The goal of this initiative is to foster a market offering greater transparency to organizations, who can then integrate this data into their risk management approach.

(source: NTIA Software Transparency website)

Problem Statement

Modern software systems involve increasingly complex and dynamic supply chains. Lack of systemic transparency into the composition and functionality of these systems contributes substantially to cybersecurity risk as well as the costs of development, procurement, and maintenance. In our highly interconnected world, increased risk and cost impact not only individuals and organizations directly but also collective goods like public safety and national security.

Increased supply chain transparency can reduce cybersecurity risks and overall costs by:

- Enhancing the identification of vulnerable systems and the root cause of incidents
- Reducing unplanned and unproductive work
- Supporting more informed free market choice of goods and encourage a positive return on investment for those companies that effectively manage their software components
- Supporting more informed market differentiation and selection
- Reducing duplication of effort by standardizing SBOM structure across multiple sectors

Thus increasing trust and trustworthiness while lowering costs of our digital infrastructure.

Pockets of people, policy, process, and technology are solving parts of the problem, but not in a systemic and scalable way that crosses development environments, product lines, vendors, sectors, and nations. A more systematic and collaborative approach can help.

Scope

The scope of this initiative will include the definition of the structure of an sBOM, how it can be shared, and how it can be used to help foster better security decisions and practices. To make the sBOM useful, this initiative will also need to outline the applicable use cases to ensure that the output is useful for all stakeholders.

All industries utilizing software should be considered in scope of this initiative, including automotive, financial, healthcare, and “traditional” IT. The focus is on software, the “S” in SBOM. We do not specifically account for hardware, however software doesn’t run by itself. A software system includes necessary hardware, including not only the necessary computing hardware but functional hardware that makes devices actually work. Cyber-physical systems?

Related Dependencies and Supporting Activities:

- Methodology for mapping vulnerabilities to components
- Stand-up of unified sharing mechanism for sBOMs
- Approach for documenting relationship between components for any given sBOM
- License management
- Lists of known vulnerabilities, exploitability, or patch level

Incorporate conceptual framing here, this is effectively definition of SBOM. Frame how Functional Objectives and Use Cases fit together using proven supply chain principles (Deming), adapted as necessary.

Learning from principles of supply chain management in other fields, we could improve knowing what software we build, acquire, operate, and depend on.