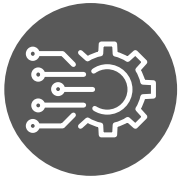
CISA SBOM Sharing Working Group - Status

February 29, 2024

Upstream open source

Vendor



Integrator

Regulator

Service Provider

Industry Association

Private Sector Information Sharing

Public Sector Information Sharing

Data Value Addition Providers

Enterprise

Enterprise Customers

“**SBOM Sharing Roles and Considerations**” - Public Mid-March

Define actors and terminology.

- **SBOM Author**: Creates an SBOM.
    - Expands “Software Producer” to include other SBOM authors.

- **SBOM Distributor**: Receives SBOMs for the purpose of sharing them with SBOM Consumers or other Distributors.
    - The role of the SBOM Distributor is a new addition to the SBOM sharing discussion. The role is introduced to capture the role of organizations that neither produce SBOMs nor make use of SBOM data.
    - Adds detail of “SBOM Provider” in CISA **SBOM Sharing Lifecycle**.

- **SBOM Consumer:** Receives the transferred SBOM. This could include roles such as third parties, authors, integrators, and end users.

“**SBOM Sharing Primer”** - Final draft shared with SBOM Working Groups

Provide practical contemporary use cases.

- Six examples of current practices:

    1. SBOMs for Proprietary Software Shared via Email
    2. SBOMs for Proprietary Software Shared via Vendor Portal
    3. SBOMs for Proprietary Software Shared via Vendor Portal with Pre-Vetting
    4. SBOM for Open Source Software (OSS) Sharing via Tooling
    5. SBOMs for OSS Share via Platform
    6. SBOMs for Proprietary Software Shared Along Supply Chain (Automotive)

Additional Use Case Documentation

- Current and potential future
- Sector specific
- End to End
- SBOM sharing objectives:security, licencing, operations, audit, …

Proof of Concept Execution

- Existing and new SBOM POCs
- ISACs, integrators, service providers, …