READ-AHEAD

# NTIA Software Component Transparency

# Healthcare Proof of Concept

Leads: Jennings Aske, New York Presbyterian; Jim Jacobson, Siemens Healthineers

## Medical Device Manufacturer* (MDM) experience (SBOM generation)

**Formats:** Both SWID and SPDX generated, slight preference for SWID (perceived as less error-prone)
**Preparation challenges:** list completeness, patch level determination, dependency relationships
**Source data:** some MDMs have central repository of components for all products, some don't
**Generation method:** various: manual, semi-automated (no automated tooling – to be developed)
**Data issues:** Product identification provided by readme – meta info that should be in the SBOM
**Future looking:** Anticipated complexity maintaining multiple version/configuration, but not covered in POC, anticipating trouble with HDOs connecting to different MDM/supplier portals

## Healthcare Delivery Organization* (HDO) experience (SBOM ingestion and use)

**CMDB:** Service Now or N/A
**Format appetite:** SPDX more human readable, SWID preferred programmatically (easier ingest)
**Data challenges:** correlation to CVEs (SBOMs should use valid CPE names), data needed to be cleaned
**Use Case Procurement** (selected individual feedback):

- System not in place to leverage SBOM in procurement
- SBOMs allowed for identification of vulnerabilities
- End-of-Life components were identified and managed via added localized programmable firewall
- Information about customized software wasn't able to be processed
- Lack of trust in the completeness of the information provided
- Missing granular patch information (e.g., for OS)

**Use Case Asset Management** (selected individual feedback):

- Digestion into CMDB not possible, tooling being developed
- Some risk management insights revealed, others are pending more sophisticated tooling
- In some cases, SBOM provided information that could be used to protect the asset
- SBOMs were useable in EoL planning, but in many cases this is still to be proven out

**Use Case Risk Management** (selected individual feedback):

- Some risk management solutions not compatible with SBOM without future 3rd- party tools
- ISO 9001 – SBOM was leveraged by providing insight into risks
- Monitoring of devices against new vulnerabilities successful, and for others possible in theory [note: PoC did not include updating SBOMs over time]

**Use Case Vulnerability Management** (selected individual feedback):

- Naming convention problem interfered
- Risk evaluation possible via associated CVSS score
- Some proactive mitigations were possible because of SBOM info

**Wishes:** CPE names, version information, patch level (at the instance), retroactive SBOMs for EoL devices

*Feedback from one MDM and one HDO pending.