Healthcare Delivery Organization (HDO)
Software Bill of Materials (SBOM)
Proof of Concept (PoC) 2.0
Quick Start Guide
V1.2

Purpose

The purpose of this “Quick Start Guide” is to provide interested parties, regardless of industry vertical, with information, experiences, and best practices related to a Software Component Transparency / Software Bill of Materials (SBOM[1]) PoC exercise. This document was developed through a working collaboration of Healthcare Delivery Organizations (HDO) and Medical Device Manufacturers (MDMs), focusing on significant developments and experiences discovered during the Healthcare SBOM PoC 1.0 (completed) and with PoC 2.0 (in progress). It is our hope that this information can be used to support the creation, sharing, ingestion, parsing, analysis, and correlation of the Software Bill of Materials (SBOM) and to provide more visibility into the security and safety of systems and applications.

1. Background Information on Healthcare Delivery Organization (HDO) Proof of Concept (PoC) 1.0

In June of 2018, the National Telecommunications and Information Administration (NTIA) engaged stakeholders from various industry verticals to address the systemic challenge of identifying, managing, and securing software components from robust and complex supply chains.

The result was the development of a formal, multi-stakeholder Software Component Transparency group, comprised of four sub-groups, with the goal of fostering a market offering with greater transparency to organizations, who can then integrate this software component data into their asset and security risk management approach.

- Framing Group
- Formats and Tooling Group
- Awareness and Adoption Group
- Healthcare Proof of Concept (PoC)

High-level information on SBOM’s background and eco-wide solution, the NTIA process, and an example of an SBOM can be accessed as part of the SBOM Two-Page Overview. Additionally, an SBOM Frequently Asked Questions (FAQ) document is available. More detailed community-drafted documentation, including the Healthcare Proof of Concept Report, are available on the broader NTIA Software Component Transparency Project site, which can be accessed via https://www.ntia.gov/SBOM.

[1] Note, the term SBOM is not to be confused with Cybersecurity Bill of Materials (CBOM), which additionally includes hardware components.

2. Legal Requirements and Non-disclosure

A requirement for the success of a PoC exercise is comprehensive data sharing across both SBOM creators (i.e. Medical Device Manufacturers) and SBOM consumers (i.e. Healthcare Delivery Organizations). An initial challenge that was faced by the working group was obtaining organizational legal approval for the disclosure of this sensitive, non-public institutional data. It was determined by the PoC Working Group that a signed non-disclosure agreement (NDA) would be required prior to the exchange of any sensitive data between the parties. It's important to note that the NDA and agreement should be protected under any current or future purchasing contracts as data sharing within the MDM and HDO was not to be used in actual contracting.

A draft NDA was routed to all of the participants' legal departments and edits were collected by a single NDA management party. Once the document was agreeable to all parties, it was routed for e-signature. Upon signature, an Internet-accessible folder share was created as a centralized collaboration space for all authorized parties. After the project commenced, additional participants were asked to sign the NDA, as written.

If an HDO or MDM would like to request participation in the ongoing Healthcare Proof of Concept 2.0, please Allan Friedman at afriedman@ntia.gov.

3. Meeting Information and Cadence

The NTIA Software Component Transparency project currently hosts a Multi-stakeholder Meeting (currently virtual only) on a quarterly basis. Information on these meetings, including previous agendas and recorded webcasts can be found at https://www.ntia.doc.gov/SoftwareTransparency. In general, the Working Groups also conduct periodic (i.e. weekly meetings) to discuss progress of key initiatives, propose solutions to identified issues, develop documentation, and manage projects within the workgroup. If you or your organization is interested in participating in the overall NTIA Software Component Transparency project or would like to join an existing workgroup, please email Allan Friedman at afriedman@ntia.gov.

4. Technologies Utilized

A number of technologies have been used to support the completion of the PoC exercises, detailed in the Use Case Exercises section below. These include, but are not limited to:

- **Internet-accessible File Sharing:** Used to exchange SBOM data and as general collaboration spaces across the MDMs and HDOs.
- **Security Incident and Event Management Software (SIEM):** Used by the HDOs to ingest the SBOM, parse out the data into additional formats, and correlate the parsed data to vulnerability information. A participating HDO has developed a SIEM Parsing Guide (*Appendix A*) to assist with the ingestion of SBOM files in the SPDX format.

- **Configuration Management Database (CMDB) or Computerized Maintenance Management System (CMMS):** Used by the HDOs to ingest the SBOM, manage software components as child assets, and leverage organizational information within the asset management systems to increase the value and usability of the SBOM data. This software can also be used to query the overall security of a fleet of systems and measure risk over time.
- **Vulnerability Scanning Engine:** The SBOM can be used to supplement existing vulnerability scanning practices (credentialed and non-credentialed) and can leverage existing vulnerability information for initial correlation. It is also plausible that a vulnerability scanning tool may be able to validate SBOM components in select use cases.
- **Enterprise Governance Risk and Compliance (eGRC) and Vendor Risk Management (VRM):** Used by the HDOs to ingest the SBOM, parse out the data, and correlate the parsed information to known vulnerabilities. eGRC and VRM technology use cases are similar to those of CMDB/CMMS; however, findings can be easily integrated into enterprise risk registers or risk management processes.
- **SOAR (Security Orchestration, Automation, and Response):** Used by HDOs to scrape the NVD site, incorporate the SBOM, and automate the collection of security threat data from multiple sources.
- **Internet of Things (IoT) / Internet of Medical Things (IoMT) Security Solutions:** Used by HDO's to monitor in real time their IoT and IoMT, which includes medical devices. Used to parse out the data and share with other tools in the security stack (such as SIEMs) or monitor in the tool for known vulnerabilities.

5. Getting Started

SBOMs can be generated using a number of formats and standards; however, the Healthcare PoC focused on two specific existing formats, Software Identification (SWID) and Software Package Data eXchange (SPDX). The high-level definition from the Standards and Formats group has been included below. Detailed information on these two formats and on SBOM production can be found in the Standards and Formats Whitepaper.

- **SWID:** A formal industry standard used by various commercial software publishers.
- **SPDX:** An open source machine-readable format stewarded as a de facto industry standard by the Linux Foundation.

See *Appendix B* for an example of the SWID SBOM syntax and format.

The selected standard must be a consensus to ensure SBOM analyses are comparable across manufacturers and devices. Once a format and generation method have been agreed upon, the participants should develop a list of in-scope systems for SBOM generation. It is the opinion of the Healthcare PoC that the initial scope should include a small, but representative sample of devices where an inventory of known software components can be reasonably obtained.

Within the Healthcare PoC, the HDOs generated a query of all production medical devices manufactured by the participating MDMs. This query included fields such as Manufacturer, Product Name, Product Type, Model Number, and Serial Number. The results of these queries were analyzed further, to identify "like" devices across the HDO system fleet. Once "like" devices had been identified, this information was provided to the MDMs for SBOM generation. SBOM generation is detailed in the Healthcare Proof of Concept Report, but in summary the following information was captured and put into both SWID and SPDX formats.

1. Author, composed of:
    a. Created By
    b. When Created
    c. Creator Comments
2. SBOM Document Name
3. List of SBOM Components, composed of the following information for each included component:
    a. Component Name
    b. Version
    c. Component Supplier
    d. Identifier
    e. Download Location
    f. Files Analyzed
    g. License
    h. Copyright Text

Subsequent SBOM generations have also included information on Persistent Uniform Resource Locator (PURL) and hierarchical component level (i.e. first level, second level, third level, etc.).

Generation of the SBOM was accomplished using both manual and automated processes, depending on the capabilities and maturity of the SBOM creator. It's possible to automatically determine the instruction set architecture (ISA) type, but there is an added benefit to determine a wider context of system deployment. Some information, such as commercial off the shelf components that were part of the build, can often be retrieved through direct software build analysis or by reviewing development documentation. Other components such as the Operating System, database, and other items included in the hardware platform may need to be obtained through other sources.

Once the SBOMs were generated, they can be securely transferred using a number of methods; however, the Healthcare PoC relied on an Internet-accessible file share. Future transmission methods include initial delivery with the device alongside the binaries, via SFTP, directly from a vendor portal, or by using an API call. Once the information has been received by the SBOM recipients, any agreed upon use case exercises can commence. The following section outlines some of the use cases that were exercised as part of the PoC 1.0 and are currently being exercised as part of PoC 2.0.

6. Use Case Exercises

Initial Data Ingestion, Parsing, and Correlation

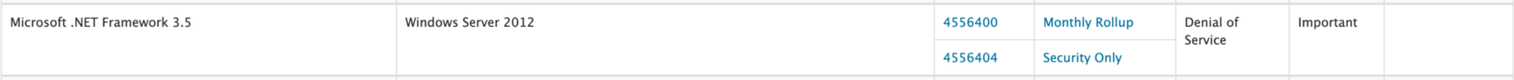
Once the SPDX SBOM has been parsed in a technology listed in Section 4 (See *Appendix A*), HDO’s also ingested data from an authoritative vulnerability source feed (i.e. National Vulnerability Database Data Feed). Similar to the SBOM, this data was parsed out in the tool using the following hierarchical schema. As an example, we will use CVE-2020-1108, a .NET Core & .NET Framework Denial of Service Vulnerability.

Parent

```
  "cve" : {
    "data_type" : "CVE",
    "data_format" : "MITRE",
    "data_version" : "4.0",
    "CVE_data_meta" : {
     "ID" : "CVE-2020-1108",
     "ASSIGNER" : "cve@mitre.org"
    },
```

Additional child data of interest may include problem type, references, description, and CVSS impact data based on the use case the SBOM consumer is exercising. Once the Parent has been defined either a cpe_match can be directly attributed to a product or in some cases, like this example showing Windows Server 2012 (Platform) and Microsoft .NET Framework 3.5 (Product), it may be attributed to a specific product and platform pairing using the AND operator.

```
"cpe_match" : [ {
      "vulnerable" : false,
      "cpe23Uri" : "cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*"
     } ]
    } ]
   }, {
    "operator" : "AND",
    "children" : [ {
     "operator" : "OR",
     "cpe_match" : [ {
      "vulnerable" : true,
      "cpe23Uri" : "cpe:2.3:a:microsoft:.net_framework:3.5:*:*:*:*:*:*:*"
     }, ...
```



Microsoft .NET Framework 3.5	Windows Server 2012	4556400 4556404	Monthly Rollup Security Only	Denial of Service	Important	

Normalization of the CPE name can then be examined to either ensure a direct match within the SIEM or implement *fuzzy logic* or *searching* to properly identify and correlate components between the SBOM and the vulnerability data. The result is a machine-readable inventory of component vulnerabilities and if desired, their related CVSS impact:

```
"impact" : {
   "baseMetricV3" : {
    "cvssV3" : {
     "version" : "3.1",
     "vectorString" : "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
     "attackVector" : "NETWORK",
     "attackComplexity" : "LOW",
     "privilegesRequired" : "NONE",
     "userInteraction" : "NONE",
     "scope" : "UNCHANGED",
     "confidentialityImpact" : "NONE",
     "integrityImpact" : "NONE",
     "availabilityImpact" : "HIGH",
     "baseScore" : 7.5,
     "baseSeverity" : "HIGH"
    },
    "exploitabilityScore" : 3.9,
    "impactScore" : 3.6
   },
   "baseMetricV2" : {
    "cvssV2" : {
     "version" : "2.0",
     "vectorString" : "AV:N/AC:L/Au:N/C:N/I:N/A:P",
     "accessVector" : "NETWORK",
     "accessComplexity" : "LOW",
     "authentication" : "NONE",
     "confidentialityImpact" : "NONE",
     "integrityImpact" : "NONE",
     "availabilityImpact" : "PARTIAL",
   "baseScore" : 5.0
  },
  "severity" : "MEDIUM",
  "exploitabilityScore" : 10.0,
  "impactScore" : 2.9,
  "acInsufInfo" : false,
  "obtainAllPrivilege" : false,
  "obtainUserPrivilege" : false,
  "obtainOtherPrivilege" : false,
  "userInteractionRequired" : false
```

Procurement

Once the SBOM data has been ingested, parsed, and is available in a standard machine-readable format (i.e. CSV), it can be manually or programmatically analyzed as part of the initial procurement process. This investigation can include the identification of known vulnerable components (see *Initial Data Ingestion, Parsing, and Correlation* section), as well as additional analyses covering end of life components, custom components, or system conflicts. Additional use cases that were explored by the HDO's were as follows:

- The development of contract language to coincide with procurement activities; in the context of the HDO PoC, this language was developed to meet cyber-security guidelines and standards promulgated by the U.S. Food and Drug Administration (FDA).
- The determination of lifecycle management processes (i.e. SBOM updates, system updates) and related contracting requirements.
- Initiate discussions for appropriate compensating controls (i.e. dynamic antivirus/antimalware, network segmentation) related to identified vulnerabilities.

In addition to the above, HDOs also explored the value of the SBOM data as part of overall pre-procurement risk activities; taking into consideration both using the SBOM as a supplemental artifact to standard pre-procurement documentation (i.e. MDS2, Vendor Questionnaires) and using the SBOM as a possible measure for the reduction of such artifacts.

Asset Management

Among the use cases for SBOMs are Asset Management. Each unique Medical Device lives in an ecosystem of other devices, and often on a network of other devices. It is important to note that although this section primarily defines asset management as the management of primary medical devices and supplemental systems, assets can also be defined as the individual software components identified in the SBOM.

Many of the industry's medical devices contain software, both unique to that Original Equipment Manufacturer (OEM) and third party. Like all software, those components have a lifecycle, and should be maintained by the component supplier until their end of life. All software contains bugs, those bugs become vulnerabilities, and a subset of those vulnerabilities will be exploitable.

Modern business entities create a list of device assets through tools such as Configuration Management Database (CMDB), or internet of things (IoT) and Internet of Medical Things (IoMt) security management tools . With an SBOM in hand for a device asset, a compiled list of software packages can be added to these asset management tools and their relationship formalized. The HDO with SBOM stored in asset management allows an organization to discover what assets have vulnerabilities. This knowledge greatly optimizes security efforts by quickly identifying affected devices.

The vulnerabilities are discovered by comparing software packages to online vulnerability sources, such as the National Vulnerability Database (NVD). The ability and desire to mitigate risk lead to several options for network hardening, and bring to attention of appropriate staff the need for software patching and updating. Occasionally, software passes into the realm of Legacy Software, software that has reached ‘end of life’ and is no longer maintained, patched, or updated. This leads to medical devices that cannot be protected via updates and may require more rigorous compensating controls against current cybersecurity threats. – (IMDRF guidance 2020). Patch management and patch tracking leave the InfoSec world when the Healthcare Technology Management (HTM) staff is called upon to take action.

The HTM department may have a separate asset management system, referred to as a Computer Maintenance Management System (CMMS). The CMMS is primarily used to manage the operational and preventative maintenance of medical devices . When updates are identified by Information Services, or in some cases HTM themselves, HTM interacts with the medical device to apply the software update in a safe manner, limiting the impact to patient care and patient safety. After mitigation of the vulnerability, hospital staff can coordinate and perform a thorough analysis of the device before returning it to clinical use.

Risk Management

Similar to *Procurement* and *Asset Management*, a number of Risk Management use cases present themselves post-ingestion of the SBOM. Once vulnerabilities have been identified, risk management systems such as an enterprise governance risk and compliance (eGRC) system can be used to register these issues, as well as measure and weigh them against organizational risk appetites and mitigating controls. Doing this enables the SBOM consumers to measure spot-in-time and trend risk across a fleet of systems, across a subset of systems, or on a system-specific level. Additional data points produced from enterprise risk assessments, machine readable MDS2’s, vulnerability scanning tools, incidents, or manual analysis can also be managed alongside the results of the SBOM analysis, providing a more holistic view into system security.

Vulnerability Management

Automated identification of system vulnerabilities can supplement existing vulnerability scanning techniques where limitations exist (e.g. unable to perform credentialed scans) and may even provide entirely novel vulnerability information in situations where systems cannot be scanned at all due to possible adverse effects on the system, such as irregular behavior. Another possibility is using binary firmware scanning for vulnerabilities. This is more of a gray box approach, and usually provides comprehensive results without affecting a running device.

It’s plausible that the vulnerability information obtained from the SBOM analysis can be ported into existing vulnerability tools to augment the current enterprise scanning results. Additional use cases include the identification of unique attack vectors for red/blue team exercises or security research proof of concept exercises. In situations where detailed vulnerability information can be obtained from existing scanning technologies, a reasonable use case involves comparing this component and vulnerability information to what is being reported on the SBOM. Such an exercise can be used as an audit function between the HDOs and the MDMs.

Once identified, vulnerabilities can be adequately managed using fixes or patches (where available), modifications to network security policies, implementing levels of microsegmentation, or other mitigation techniques to reduce the risk until a permanent solution can be applied. Wherever possible, the installation of heuristic analysis tools may also be able to detect unauthorized activity before exploitability is discovered in the wild.

Conclusion

An SBOM PoC exercise does not need to include or be limited to the technologies and use-cases described throughout this document to be successful. The information above was developed primarily to serve as a general guide, documenting the experience of the Healthcare Proof of Concept working group.

Throughout the project, the participating MDMs and HDOs have achieved success through frequent communication and information sharing, continuous improvement, and the ongoing examination of available tools and technologies. Looking forward, participants have opted into a phased approach for the second PoC, breaking up known issues and challenges into separate project sprints. We expect to develop a successive report detailing this approach as a “Healthcare Proof of Concept 2.0” document, available in 2021.

Appendix A – SIEM Parsing Guide

This is a high-level guide describing how SBOM SPDX files were parsed by a participating HDO Team.

1. The SPDX SBOM file uses a multiline format and it is delimited by string “PackageName:”
2. The first SIEM “event” is the header. The timestamp used in most SIEM solutions can be extracted from this header.
3. Each Package is also considered an event, but doesn’t contain a timestamp. To facilitate this, the HDO configured these events to inherit the timestamp from the header, which is the first event of the file. Note, some SIEM tools will use the timestamp from the previous event if the current event doesn’t contain a timestamp.
4. After being delimited by the string “PackageName:”, each event becomes a long string/line. Therefore, regex is used to extract each field.
5. If the order of some of the fields were to shift, the regex below will not work and will need to be modified. As such, it’s important that the SPDX file format remains consistent. After analyzing the SPDX files provided by the MDMs in PoC 2.0, the participating HDO made some modifications to help ingest SBOM SPDX files with slight format inconsistencies. For example, one of the sample files had a comment section that had field and value pairs in it. As such, regex was updated to ignore a field that starts with #.
6. Below is the regex used to extract the fields from the SPDX file. This was tested with the SBOM SPDX files used in the Healthcare Proof of Concept and worked as expected.

```
SPDXVersion = (?<!#)\s+SPDXVersion:\s+(?<SPDXVersion>.+)\s+DataLicense
DataLicense = (?<!#)\s+DataLicense:\s+(?<DataLicense>.+)\s+SPDXID
SPDXID-DOC = (?<!#)\s+SPDXID:\s+(?<SPDXID>.+)\s+DocumentName:
DocumentName = (?<!#)\s+DocumentName:\s+(?<DocumentName>.+)\s+DocumentNamespace
DocumentNamespace = (?<!#)\s+DocumentNamespace:\s+(?<DocumentNamespace>\S+)
Creator-Organization = (?<!#)\s+Creator:\s+Organization:\s+(?<Creator_Organization>.+?)\s+(Creator:|Created:)
Creator-Person = (?<!#)\s+Creator:\s+Person:\s+(?<Creator_Person>.+?)\s+(Creator:|Created:)
Creator-Tool = (?<!#)\s+Creator:\s+Tool:\s+(?<Creator_Tool>.+?)\s+(Creator:|Created:)
CreatorComment = (?<!#)\s+CreatorComment:\s+<text>(?<CreatorComment>.+)</text>
PackageName = (?<!#)(?<PackageName>.+)(?<!#)\s+SPDXID.+PackageComment
SPDXID = (?<!#)\s+SPDXID:\s+(?<SPDXID>.+)\s+PackageComment
PackageComment = (?<!#)\s+PackageComment:\s+<text>(?<PackageComment>.+)</text>
PackageVersion = (?<!#)\s+PackageVersion:\s+(?<PackageVersion>.+)\s+PackageSupplier
PackageSupplier = (?<!#)\s+PackageSupplier:\s+((Organization:\s+)|)(?<PackageSupplier>.+)\s+Relationship
Relationship = (?<!#)\s+Relationship:\s+(?<Relationship>.+)\s+PackageDownloadLocation
PackageDownloadLocation = (?<!#)\s+PackageDownloadLocation:\s+(?<PackageDownloadLocation>.+)\s+FilesAnalyzed
FilesAnalyzed = (?<!#)\s+FilesAnalyzed:\s+(?<FilesAnalyzed>.+)\s+PackageLicenseConcluded
PackageLicenseConcluded = (?<!#)\s+PackageLicenseConcluded:\s+(?<PackageLicenseConcluded>.+)\s+PackageLicenseDeclared
PackageLicenseDeclared = (?<!#)\s+PackageLicenseDeclared:\s+(?<PackageLicenseDeclared>.+)\s+PackageCopyrightText
PackageCopyrightText = (?<!#)\s+Packag+eCopyrightText:\s+(?<PackageCopyrightText>.+?)\s+(#|)
```

Appendix B – Example SWID SBOM (ACME Corporation Road Runner Detector)

```
<SoftwareIdentity
xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd" name="ACME
Roadrunner Detector 2013 Coyote Edition SP1"tagId="com.acme.rrd2013-ce-sp1-v4-1-
5-0" version="4.1.5">
    <Entity name="The ACME Corporation" regid="acme.com" role="tagCreator
    softwareCreator"/>
    <Link rel="license" href="www.gnu.org/licenses/gpl.txt"/>
    <Meta product="Roadrunner Detector" colloquialVersion="2013"
    edition="coyote" revision="sp1"/>
    <Payload>
        <File name="rrdetector.exe" size="532712"
        SHA256:hash="a314fc2dc663ae7a6b6bc6787594057396e6b3f569
        cd50fd5ddb4d1bbafd2b6a"/>
</Payload>
</SoftwareIdentity>
```