Software Bill Of Materials
Overview

Charlie Hart
Hitachi America R&D
Uptane Software Supply Chain Workshop
March 31, 2023
Software Bill of Materials Overview

What is an SBOM?
Why are SBOMs needed and what is driving them?
SBOM details
Auto-ISAC SBOM Working Group
Exchanging SBOMs
What Is a Software Bill of Materials (SBOM)

SBOM: A formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships.

- Comprehensive inventory (or explicitly state where it is not)
- May include open source or proprietary software
- Can be widely or publicly available, or access-restricted

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Supplier Name</th>
<th>Version String</th>
<th>Author</th>
<th>Hash</th>
<th>UID</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Acme</td>
<td>1.1</td>
<td>Acme</td>
<td>0x123</td>
<td>234</td>
<td>Self</td>
</tr>
<tr>
<td></td>
<td>--- Browser</td>
<td>Bob</td>
<td>2.1</td>
<td>Bob</td>
<td>0x223</td>
<td>334</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--- Compression</td>
<td>Carol</td>
<td>3.1</td>
<td>Acme</td>
<td>0x323</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--- Buffer</td>
<td>Bingo</td>
<td>2.2</td>
<td>Acme</td>
<td>0x423</td>
</tr>
</tbody>
</table>

History:
2018: FDA-mandated security improvements.
2019, 2021: DoC NTIA guidance
2021: Required by USG and others
2022: Auto-ISAC Practice guidance

Key points for automotive industry
1. Applies to embedded software, firmware, and microcode
2. Important aspect of safety for technology supply chain
Infrastructure Companies Say Suppliers Pose a Growing Cyber Threat

Regulators should look closely at the companies supplying critical infrastructure operators, security chiefs say.

Companies in critical infrastructure sectors say weak cyber defenses at suppliers are becoming a significant threat to their business, and that rules to boost security down the supply chain might be needed.

While federal and industry rules for specific areas such as aviation, pipeline companies and other critical infrastructure operators are well-established, said Curley Henry, vice president and deputy chief information security officer at power utility Southern Co., cyber

“The supply chain is the area where the threats are growing the most for us, but the regulations aren’t targeted to those who are providing the products,” Mr. Henry said, speaking on a virtual panel hosted Thursday by industrial cybersecurity firm Dragos Inc.
GitHub says hackers cloned code-signing certificates in breached repository

It remains unclear how the threat actor compromised access token used in the breach.

DAN GOODIN - 1/30/2023

GitHub said unknown intruders gained unauthorized access to some of its code repositories and stole code-signing certificates for two of its desktop applications: Desktop and Atom.

Code-signing certificates place a cryptographic stamp on code to verify it was developed by the listed organization, which in this case is GitHub. If decrypted, the certificates could allow an attacker to sign unofficial versions of the apps that had been maliciously tampered with and pass them off as legitimate updates from GitHub. Current versions of Desktop and Atom are unaffected by the credential theft.
ChatGPT Data Breach Confirmed as Security Firm Warns of Vulnerable Component Exploitation

OpenAI has confirmed a ChatGPT data breach on the same day a security firm reported seeing the use of a component affected by an actively exploited vulnerability.

The issue was related to ChatGPT’s use of Redis-py, an open source Redis client library, and it was introduced by a change made by OpenAI on March 20.
What is driving adoption of SBOMs?

May 2021 - Executive Order 14028 – “Improving the Nation’s Cybersecurity”
What Can and Can’t SBOMs Do?

SBOMs CAN:
- Assist in Incident Response by saving a lot of evaluation time and effort
- Quickly identify compromised open source/3rd party modules that are otherwise hidden in a software program
- Verify that software is free of vulnerabilities before purchase
- Be stored in CMDB or software asset databases for easy reference

SBOMs CAN’T:
- Provide protection without other tools or interventions
- Replace EDR, SoC, or other security measures
- Be a source of threat intelligence before a vulnerability is revealed
# What Makes a Trusted Partner?

<table>
<thead>
<tr>
<th>Outside Influences</th>
<th>Company</th>
<th>Operations</th>
<th>Production</th>
<th>Product</th>
<th>Negative Influences</th>
</tr>
</thead>
<tbody>
<tr>
<td>regulation</td>
<td>vision</td>
<td>security</td>
<td>safety</td>
<td>reliability</td>
<td>hazards</td>
</tr>
<tr>
<td>market</td>
<td>strategy</td>
<td>privacy</td>
<td>security</td>
<td>performance</td>
<td>threats</td>
</tr>
<tr>
<td>political</td>
<td>ownership</td>
<td>financial</td>
<td>resilience</td>
<td>quality</td>
<td>disturbances</td>
</tr>
<tr>
<td>society</td>
<td>business model</td>
<td>procurement</td>
<td>standards</td>
<td>suitability</td>
<td>human errors</td>
</tr>
<tr>
<td>standards</td>
<td>success</td>
<td>logistic</td>
<td>techniques</td>
<td></td>
<td>faults</td>
</tr>
<tr>
<td>competition</td>
<td>reputation</td>
<td>support</td>
<td>processes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>technology</td>
<td>culture</td>
<td>compliance</td>
<td>data logging</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>location</td>
<td>suppliers</td>
<td>auditability</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>political/legal</td>
<td>customers</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*From Industrial Internet Consortium: “Trustworthiness Framework Foundations,” 2021-05-27*
NIST C-SCRM – Executive Order 14028 – “Software Supply Chain Security”

EO Section 4 Tasks and Timelines

- **Day 0 – May 12, 2021**
  - EO 14028 issued

- **Day 45 – June 26, 2021**
  - Publish definition of “critical software” (4a)

- **Day 60 – July 11, 2021**
  - Publish guidance outlining security measures for critical software (4i)

- **Day 60 – July 11, 2021**
  - Publish guidelines recommending minimum standards for vendor testing of SW source code (4r)

- **Day 180 – Nov 8, 2021**
  - Publish preliminary guidelines for enhancing SW SC security (4c)

- **Day 360 – May 8, 2022**
  - Publish additional guidelines, including review/update procedures (4d)

- **Day 360 – May 8, 2022**
  - Issue guidance identifying practices that enhance security of SW SC (4e)

- **Day 365 – May 13, 2022**
  - Initiate pilot programs, identifying IoT cyber & secure SW development practices or criteria for consumer labeling programs (4s, 4t, 4u)

- **Day 365 – May 13, 2022**
  - Review & submit summary report of pilot programs (4w)
NIST SSDF – Executive Order 14028 – “Consumer Labeling”

**EO Section 4 Tasks and Timelines**

- **Day 0 – May 12, 2021**
  - EO 14028 issued

- **Day 30 – June 11, 2021**
  - Solicit input from stakeholders (4b)

- **Day 45 – June 26, 2021**
  - Publish definition of “critical software” (4g)

- **Day 60 – July 11, 2021**
  - Publish guidance outlining security measures for critical software (4i)

- **Day 180 – Nov 8, 2021**
  - Publish preliminary guidelines for enhancing SW SC security (4c)

- **Day 360 – May 8, 2022**
  - Publish additional guidelines, including review/update procedures (4d)

- **Day 365 – May 13, 2022**
  - NIST Supply Chain Guidance
  - Summary report of pilot programs (4w)

Issue guidance identifying practices that enhance security of SW SC (4e)
Initiate pilot programs, identifying IoT cyber & Secure SW development practices or criteria for consumer labeling programs (4s, 4t, 4u)

**Day 270 – Feb 6, 2022**
NIST SSDF – Executive Order 14028 – ” Consumer Labeling”

• Goals:
  • Public disclosure on cybersecurity (up to a point?)
  • IoT and OT devices/products
  • Development processes (i.e. pedigree) – includes full security over dev/build systems

• Tactics
  • Incentives for participation by IoT and OT vendors
  • Integrity, quality/test, and security practice attestations and artifacts
  • Federal purchases
  • Handy spreadsheet here: https://csrc.nist.gov/csrc/media/Publications/sp/800-218/final/documents/NIST.SP.800-218.SSDF-table.xlsx
RECOMMENDED CRITERIA FOR CYBERSECURITY LABELING
FOR CONSUMER IOT PRODUCTS

Asset identification - product and subcomponents/SBOM

Product Configuration - customer controls

Data Protection

Interface Access Control - includes MFA, zero trust

Software update

Cybersecurity state awareness (logging)

Information and Query Reception (comms between cust/support parties and devs)

Info Dissemination (terms of support incl. sw update frequency/mechs, EOL, reqs for maintenance, breach disclosure and mitigation)

Product Education and Awareness (cybersec capability/instructions)

Documentation
- Design assumptions (use cases, audience/users, network access, data, cyber requirements, laws/regs, lifespan), components,
- Baseline product criteria met/not met (and why if not).
- Product design and support considerations (3rd party/OSS components, platform, protection mechs, known risks, secure dev/SSC practices used, certs/evals for cyber, install/maint usability)
- Maint req’s incl. authorized support parties
- Secure system lifecycle policies (how prod is ensured to have no known exploitable vulns, lifecycle maintenance of underlying components, dealing with pre- and post-EOL vulns/defects)
RECOMMENDED CRITERIA FOR CYBERSECURITY LABELING FOR CONSUMER IOT PRODUCTS

Asset identification - product and subcomponents/SBOM

Product Configuration - customer controls

Data Protection

Interface Access Control - includes MFA, zero trust

Software update

Cybersecurity state awareness (logging)

Information and Query Reception (comms between cust/support parties and devs)

Info Dissemination (terms of support incl. sw update frequency/mechs, EOL maintenance, breach disclosure and mitigation)

Product Education and Awareness (cybersec capability/instructions)

Documentation

• Design assumptions (use cases, audience/users, network access, data, cyber requirements, laws/regs, lifespan), components

• Baseline product criteria met/not met (and why if not).

• Product design and support considerations (3rd party/OSS components, platform, protection mechs, known risks, secure dev/SSC practices used, certs/evals for cyber, install/maint usability)

• Maint req’s incl. authorized support parties

• Secure system lifecycle policies (how prod is ensured to have no known exploitable vulns, lifecycle maintenance of underlying components, dealing with pre- and post-EOL vulns/defects)
Supply Chain Levels for Software Artifacts (SLSA) - Basic Map of SDLC
SLSA – Basic Map

- **Source Integrity**
  - Compromise source control (B)
  - Submit bad code (A)

- **Build Integrity**
  - Compromise build platform (D)
  - Modify code (C)
  - Use bad dependency (E)
  - Bypass CI/CD (F)
  - Compromise package repository (G)

- **Distribution**
  - Use bad package (H)

- **Use**

**SBOM**
Software Bill of Materials (SBOM)

SBOM: A formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships.

- Comprehensive inventory (or explicitly state where it is not)
- May include open source or proprietary software
- Can be widely or publicly available, or access-restricted

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Supplier Name</th>
<th>Version String</th>
<th>Author</th>
<th>Hash</th>
<th>UID</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Acme</td>
<td>1.1</td>
<td>Acme</td>
<td>0x123</td>
<td>234</td>
<td>Self</td>
</tr>
<tr>
<td>--- Browser</td>
<td>Bob</td>
<td>2.1</td>
<td>Bob</td>
<td>0x223</td>
<td>334</td>
<td>Included in</td>
</tr>
<tr>
<td>--- Compression Engine</td>
<td>Carol</td>
<td>3.1</td>
<td>Acme</td>
<td>0x323</td>
<td>434</td>
<td>Included in</td>
</tr>
<tr>
<td>--- Buffer</td>
<td>Bingo</td>
<td>2.2</td>
<td>Acme</td>
<td>0x423</td>
<td>534</td>
<td>Included in</td>
</tr>
</tbody>
</table>

History:
2018: FDA-mandated security improvements.
2019, 2021: DoC NTIA guidance
2021: Required by USG and others
2022: Auto-ISAC Practice guidance

Key points for automotive industry
1. Applies to embedded software, firmware, and microcode
2. Important aspect of safety for technology supply chain
## SBOM Baseline Data v2.0 - “Minimum Viable Product” + Timestamp

<table>
<thead>
<tr>
<th><strong>Author Name</strong></th>
<th>Author of the SBOM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supplier Name</strong></td>
<td>The entity who is responsible for support of the object of the SBOM. Vendor, Manufacturer, Developer, Maintainer, Distributor, etc.</td>
</tr>
<tr>
<td><strong>Component Name</strong></td>
<td>Supplier or Author decides</td>
</tr>
<tr>
<td><strong>Version String</strong></td>
<td>Supplier decides</td>
</tr>
<tr>
<td><strong>Component Hash (Optional)</strong></td>
<td>Cryptographic code check to ensure component matches SBOM references. Desirable but sometimes difficult to implement.</td>
</tr>
<tr>
<td><strong>Unique Identifier</strong></td>
<td>CPE, purl, UUID, GUID, etc</td>
</tr>
<tr>
<td><strong>Relationship</strong></td>
<td>“Self” is the component that is the subject of the SBOM. ”Included in” references another SBOM component.</td>
</tr>
<tr>
<td><strong>Creation time/date</strong></td>
<td>For disambiguation in the rare event of multiple SBOM versions.</td>
</tr>
</tbody>
</table>
Cyclone DX (XML): Cisco AMP/Android

SBOM: Cisco AMP Endpoint for Android (CycloneDX format)
SPDX (Proprietary Format): Cisco AMP/Android (1/2)

## Packages

### 2.4 Primary Component (described by the SBOM)

**PackageName:** Cisco Secure Endpoints for Android  
**SPDXID:** SPDXRef-Cisco-Secure-Endpoints-for-Android  
**PackageComment:**  
**ExternalRef:** PACKAGE-MANAGER purl pkg:supplier/Cisco/Cisco%20Secure%20Endpoints%20for%20Android@2.1.0  
**PackageVersion:** 2.1.0  
**PackageSupplier:** Organization: Cisco  
**Relationship:** SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS NONE  
**PackageDownloadLocation:** https://software.cisco.com/  
**FilesAnalyzed:** true  
**PackageLicenseConcluded:** NOASSERTION  
**PackageLicenseDeclared:** NOASSERTION  
**PackageCopyrightText:** NOASSERTION  

### 2.4 All-Levels Components

**PackageName:** okhttp  
**SPDXID:** SPDXRef-okhttp  
**PackageComment:**  
**ExternalRef:** PACKAGE-MANAGER purl pkg:supplier/Square/okhttp@4.2.2  
**PackageVersion:** 4.2.2  
**PackageSupplier:** Organization: Square  
**Relationship:** SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS SPDXRef-okhttp  
**PackageDownloadLocation:** https://github.com/square/okhttp  
**FilesAnalyzed:** false  
**PackageLicenseConcluded:** NOASSERTION  
**PackageLicenseDeclared:** NOASSERTION  
**PackageCopyrightText:** NOASSERTION  
**PackageHomePage:** https://square.github.io/okhttp/  

### 2.4 All-Levels Components

**PackageName:** design  
**SPDXID:** SPDXRef-design-  
**PackageComment:**  
**ExternalRef:** PACKAGE-MANAGER purl pkg:supplier/design/design%20@2.0.3  
**PackageVersion:** 2.0.3  
**PackageSupplier:** Organization: design  
**Relationship:** SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS SPDXRef-design-  
**PackageDownloadLocation:** NOASSERTION  
**FilesAnalyzed:** true  
**PackageLicenseConcluded:** NOASSERTION  
**PackageLicenseDeclared:** NOASSERTION  
**PackageCopyrightText:** NOASSERTION  

Continued next page...
## 2.4 All-Levels Components

### bouncy-castle

**SPDXID:** SPDXRef-bouncy-castle

**PackageComment:** `<text>PURL is pkg:supplier/Bouncy%20Castle/bouncy-castle@1.62.0</text>`

**ExternalRef:** PACKAGE-MANAGER purl pkg:supplier/Bouncy%20Castle/bouncy-castle@1.62.0

**PackageVersion:** 1.62.0

**PackageSupplier:** Organization: Bouncy Castle

**Relationship:** SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS SPDXRef-bouncy-castle

**Relationship:** SPDXRef-bouncy-castle CONTAINS NOASSERTION

**PackageDownloadLocation:** https://www.bouncycastle.org/latest_releases.html

**FilesAnalyzed:** true

**PackageLicenseConcluded:** NOASSERTION

**PackageLicenseDeclared:** NOASSERTION

**PackageCopyrightText:** NOASSERTION

**PackageHomePage:** https://www.bouncycastle.org

### xmlsec-java

**SPDXID:** SPDXRef-xmlsec-java

**PackageComment:** `<text>PURL is pkg:supplier/Apache%20Santuario/xmlsec-java@2.1.4</text>`

**ExternalRef:** PACKAGE-MANAGER purl pkg:supplier/Apache%20Santuario/xmlsec-java@2.1.4

**PackageVersion:** 2.1.4

**PackageSupplier:** Organization: Apache Santuario

**Relationship:** SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS SPDXRef-xmlsec-java

**Relationship:** SPDXRef-xmlsec-java CONTAINS NOASSERTION

**PackageDownloadLocation:** https://santuario.apache.org/download.html

**FilesAnalyzed:** false

**PackageLicenseConcluded:** NOASSERTION

**PackageLicenseDeclared:** NOASSERTION

**PackageCopyrightText:** NOASSERTION

**PackageFileName:** xmlsec-2.1.4-source-release.zip

**PackageHomePage:** https://santuario.apache.org

NOTE: Not for official use – for illustration purposes only. Edited for brevity - Apache License text removed.
Cyclone DX (XML): Cisco AMP/Android

```xml
<?xml version="1.0"?>
<bom xmlns="urn:uuid:lec1d9-3bad-4cb6-f451-053220fbc0a" version = "1" xmlns="http://cyclonedx.org/schema/bom/1.2">
    <metadata>
        <timestamp>2021-06-11T01:35:00Z</timestamp>
        <authors>
            <author>
                <name>Omar Santos</name>
                <email></email>
            </author>
        </authors>
        <components type="device" bom-ref="24a36030-1f36-f9b7-e303-911fd1756c3">
            <name>Cisco Secure Endpoints for Android</name>
            <version>2.1.0</version>
        </component>
        <components type="library" bom-ref="c639e5f9-557d-e679-1a76-5f70c146feaa">
            <name>Jetty</name>
            <version>9.4.15.v20161018</version>
        </component>
        <components type="library" bom-ref="c99835f9-557d-e679-1a76-5f70c146feaa">
            <name>OkHttp</name>
            <version>3.14.1</version>
        </component>
    </metadata>
</bom>
```

SBOM Header Fields

SBOM: Cisco AMP Endpoint for Android (CycloneDX format)
Cyclone DX (XML): Cisco AMP/Android

SBOM Components

SBOM: Cisco AMP Endpoint for Android (CycloneDX format)
Cyclone DX (XML): Cisco AMP/Android

SBOM: Cisco AMP Endpoint for Android (CycloneDX format)
NOTE: Not for official use – for illustration purposes only. Edited for brevity - Apache License text removed.
## 2.4 Primary Component (described by the SBOM)
### PackageName: Cisco Secure Endpoints for Android
SPDXID: SPDXRef-Cisco-Secure-Endpoints-for-Android
PackageComment:  <text>PURL is pkg:supplier/Cisco/Cisco%20Secure%20Endpoints%20for%20Android@2.1.0</text>
ExternalRef: PACKAGE-MANAGER purl pkg:supplier/Cisco/Cisco%20Secure%20Endpoints%20for%20Android@2.1.0
PackageVersion: 2.1.0
PackageSupplier: Organization: Cisco
Relationship: SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS NONE
PackageDownloadLocation: https://software.cisco.com/
FilesAnalyzed: true
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION

### 2.4 All-Levels Components
#### PackageName: okhttp
SPDXID: SPDXRef-okhttp
PackageComment: <text>PURL is pkg:supplier/Square/okhttp@ 4.2.2</text>
ExternalRef: PACKAGE-MANAGER purl pkg:supplier/Square/okhttp@ 4.2.2
PackageVersion: 4.2.2
PackageSupplier: Organization: Square
Relationship: SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS SPDXRef-okhttp
PackageDownloadLocation: https://github.com/square/okhttp
FilesAnalyzed: false
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageHomePage: https://square.github.io/okhttp/

#### PackageName: design
SPDXID: SPDXRef-design-
PackageComment: <text>PURL is pkg:supplier/design/design%20@2.0.3</text>
ExternalRef: PACKAGE-MANAGER purl pkg:supplier/design/design%20@2.0.3
PackageVersion: 2.0.3
PackageSupplier: Organization: design
Relationship: SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS SPDXRef-design-
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: true
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION

Continued next page...
### Document Header
- **SPDXVersion:** SPDX-2.1
- **DataLicense:** CC0-1.0
- **SPDXID:** SPDXRef-DOCUMENT
- **DocumentName:** CISCO-AMP-ENDPOINTS-ANDROID-DRAFT
- **DocumentNamespace:** https://www.cisco.com/spdxdocs
- **Creator:** Person: Omar Santos
- **Created:** 2021-06-11T01:35:00Z
- **CreatorComment:** <text>DRAFT - DEMO ONLY - SBOM of Cisco AMP for Endpoints Connector for Android 2.1.0
THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.</text>

### Packages

#### 2.4 Primary Component (described by the SBOM)
- **PackageName:** Cisco Secure Endpoints for Android
- **SPDXID:** SPDXRef-Cisco-Secure-Endpoints-for-Android
- **PackageComment:** <text>PURL is pkg:supplier/Cisco/Cisco%20Secure%20Endpoints%20for%20Android@2.1.0</text>
- **ExternalRef:** PACKAGE-MANAGER purl pkg:supplier/Cisco/Cisco%20Secure%20Endpoints%20for%20Android@2.1.0
- **PackageVersion:** 2.1.0
- **PackageSupplier:** Organization: Cisco
- **Relationship:** SPDXRef-DOCUMENT DESCIBES SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS NONE
- **PackageDownloadLocation:** https://software.cisco.com/
- **FilesAnalyzed:** true
- **PackageLicenseConcluded:** NOASSERTION
- **PackageLicenseDeclared:** NOASSERTION
- **PackageCopyrightText:** NOASSERTION

#### 2.4 All-Levels Components

##### 2.4.1 Components

- **PackageName:** okhttp
- **SPDXID:** SPDXRef-okhttp
- **PackageComment:** <text>PURL is pkg:supplier/Square/okhttp@ 4.2.2</text>
- **ExternalRef:** PACKAGE-MANAGER purl pkg:supplier/Square/okhttp@ 4.2.2
- **PackageVersion:** 4.2.2
- **PackageSupplier:** Organization: Square
- **Relationship:** SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS SPDXRef-okhttp
- **PackageDownloadLocation:** https://github.com/square/okhttp
- **FilesAnalyzed:** false
- **PackageLicenseConcluded:** NOASSERTION
- **PackageLicenseDeclared:** NOASSERTION
- **PackageCopyrightText:** NOASSERTION
- **PackageHomePage:** https://square.github.io/okhttp/

##### 2.4.2 Components

- **PackageName:** design
- **SPDXID:** SPDXRef-design
- **PackageComment:** <text>PURL is pkg:supplier/design/design@2.0.3</text>
- **ExternalRef:** PACKAGE-MANAGER purl pkg:supplier/design/design@2.0.3
- **PackageVersion:** 2.0.3
- **PackageSupplier:** Organization: design
- **Relationship:** SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS SPDXRef-design
- **PackageDownloadLocation:** NOASSERTION
- **FilesAnalyzed:** true
- **PackageLicenseConcluded:** NOASSERTION
- **PackageLicenseDeclared:** NOASSERTION
- **PackageCopyrightText:** NOASSERTION
SBOM Creation and Maintenance

SBOMS can be generated at any phase of the Development Lifecycle
- During development – manual or via dev workbench
- During build (preferred)
- Post-Build SCA/ECA tool/audit by supplier or customer
- Run-time – IAST/RASP, Mobile

1. SBOMs should be generated at build time for the most authoritative information
2. SBOMs are valid only for the specific software each one describes
3. SBOMs need to be created whenever software is updated
AutoISAC SBOM Working Group - History

**Phase 1 – Mar-Jul 2019**

**Sponsor:** Analyst WG

**Goal:** Ensure NTIA SBOM considers automotive industry issues and opinions

**Team:** 10 members (includes 3 OEMs)

**Objective:** Publish concerns to NTIA and advocate for the auto industry

**Phase 2 – Nov 2020 – Dec 2021**

**Sponsor:** Supplier Affinity Group

**Goal:** Agree on best practices among suppliers and propose solution to OEMs

**Team:** 17 members (1 OEM)

**Objectives:**
- Unified supplier voice on SBOM adoption to OEMs
- Align with NTIA
- Practical approach with input from OEMs
- Best Practice published in 2021
AutoISAC SBOM Working Group – History (2/2)

Phase 3 – July 2022 - Present

**Sponsor:** Board of Directors

**Goal:** Exercise proposed solutions, fully involve OEMs

**Team:** 38 members (13 OEMs, 25 Suppliers)

**Objectives:**
- Plan exercises
- Agree on SBOM samples for exercises in detail
- Iterate TTXs
- Iterate live exercises
- Pilot in production (aspirational)
- Final report to Board of Directors
1. What info is needed on an SBOM to provide analysis, sharing guidance, and security?
2. What info is shared with consumers of the component?
3. How are components classified in an SBOM?
4. How are components identified, e.g. version, branch, fragment, supplier/author?
5. What is the balance between transparency vs. liability?
6. How can IP be protected in a transparent BOM?
7. Should a BOM enumerate all variations?
8. Who gets the SBOM and by what means?
9. How can subcomponents of large libraries be distinguished from general use of the library?
10. How will AutoISAC interact with and influence other SBOM projects?
11. How will components be identified, tracked, and audited by the consumer of the component?
12. How will software engineering and QA teams provide SBOMs?
13. How will purchasing agents enforce SBOM best practice and block restricted components?
Phase 2 Findings Report

**INCLUDES**
- distribution (for now)
- Substantial overlap with NTIA guidance
- Customizations for automotive
- Mapping to automotive product lifecycle
- Format and operational recommendations
- Sharing discussion
- Vendor-neutral tool list
- Bibliography, training, and reference docs

**WILL NOT INCLUDE**
- Mandatory rules – all points will be recommendations
- Usurpation of supplier contracts or requirements
- Static guidance – revisions expected during Phase 3 and ongoing
Exchanging SBOMs

- IETF Manufacturers Usage Definition (MUD)
- IETF SCITT - [https://github.com/ietf-scitt/scitt-web](https://github.com/ietf-scitt/scitt-web)
- DBOM - decentralized approach to sharing with a policy base
- Trust Store (Hitachi)
- Email, ftp,
- Software installation kits
- Industry/vendor/supplier portals
- Manufacturer Disclosure Statement for Medical (MDS2) form (2019)
- ISAC e.g. [https://h-isac.org/tag/sbom/](https://h-isac.org/tag/sbom/)
- MISP Threat Sharing [https://www.misp-project.org/](https://www.misp-project.org/)
- OpenC2
- Commercial products - cybersecurity, supply chain, secure document exchange
- **OTA??**
Thank you! Questions?