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

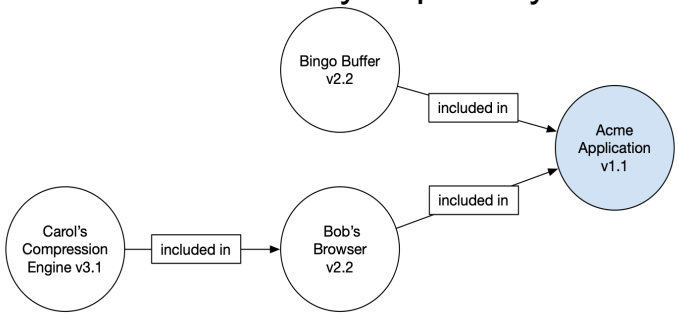
Auto-ISAC SBOM Working Group

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



Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Self
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

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**

News – January 27, 2023

WSJ PRO CYBERSECURITY

Home News Research Newsletters Events Search

SHARE

WSJ PRO

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.

Cybersecurity news, analysis and insights from WSJ's global team of reporters and editors.

that needs to get a lot of focus," he said.

News – January 30, 2023

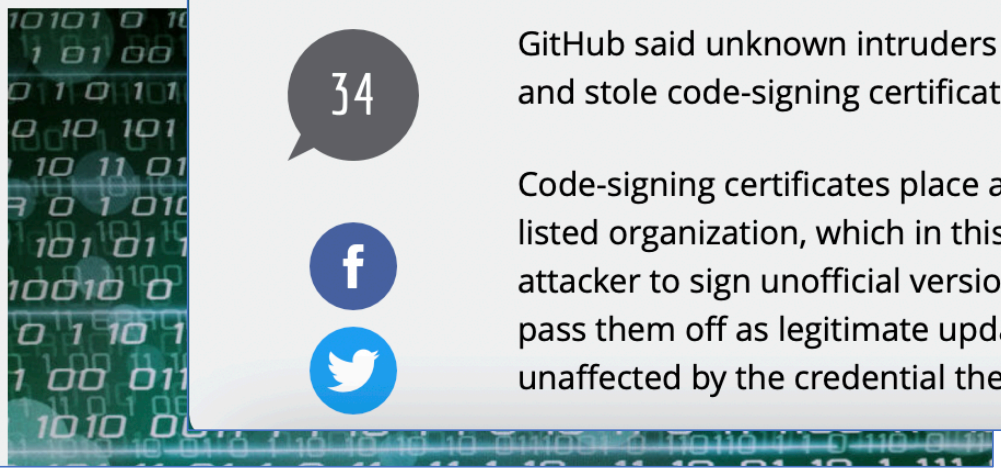
ars TECHNICA

BEWARE ... CERTIFICATE REVOCATIONS AHEAD —

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



34

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.

News – March 28, 2023

DATA BREACHES

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.

By Eduard Kovacs
March 28, 2023

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

TRENDING

1 Chrome 111 Update Patches High-Severity Vulnerabilities
2 ChatGPT Data Breach Confirmed as Security Firm Warns of Vulnerable Component Exploitation
3 Microsoft: No-Interaction Outlook Zero Day Exploited Since Last April

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.

OpenAI said on Friday that it had taken the chatbot offline earlier in the week while it worked with the maintainers of the Redis data platform to patch a flaw that resulted in the exposure of user information.

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.

The chatbot's developers use Redis to cache user information in their server, to avoid having to check the database for every request. The Redis-py library serves as a Python interface.

The bug introduced by OpenAI resulted in ChatGPT users being shown chat data belonging to others.

According to OpenAI's investigation, the titles of active users' chat history and the first message of a newly created conversation were exposed in the data breach. The bug also exposed payment-related information belonging to 1.2% of ChatGPT Plus

Daily Briefing Newsletter

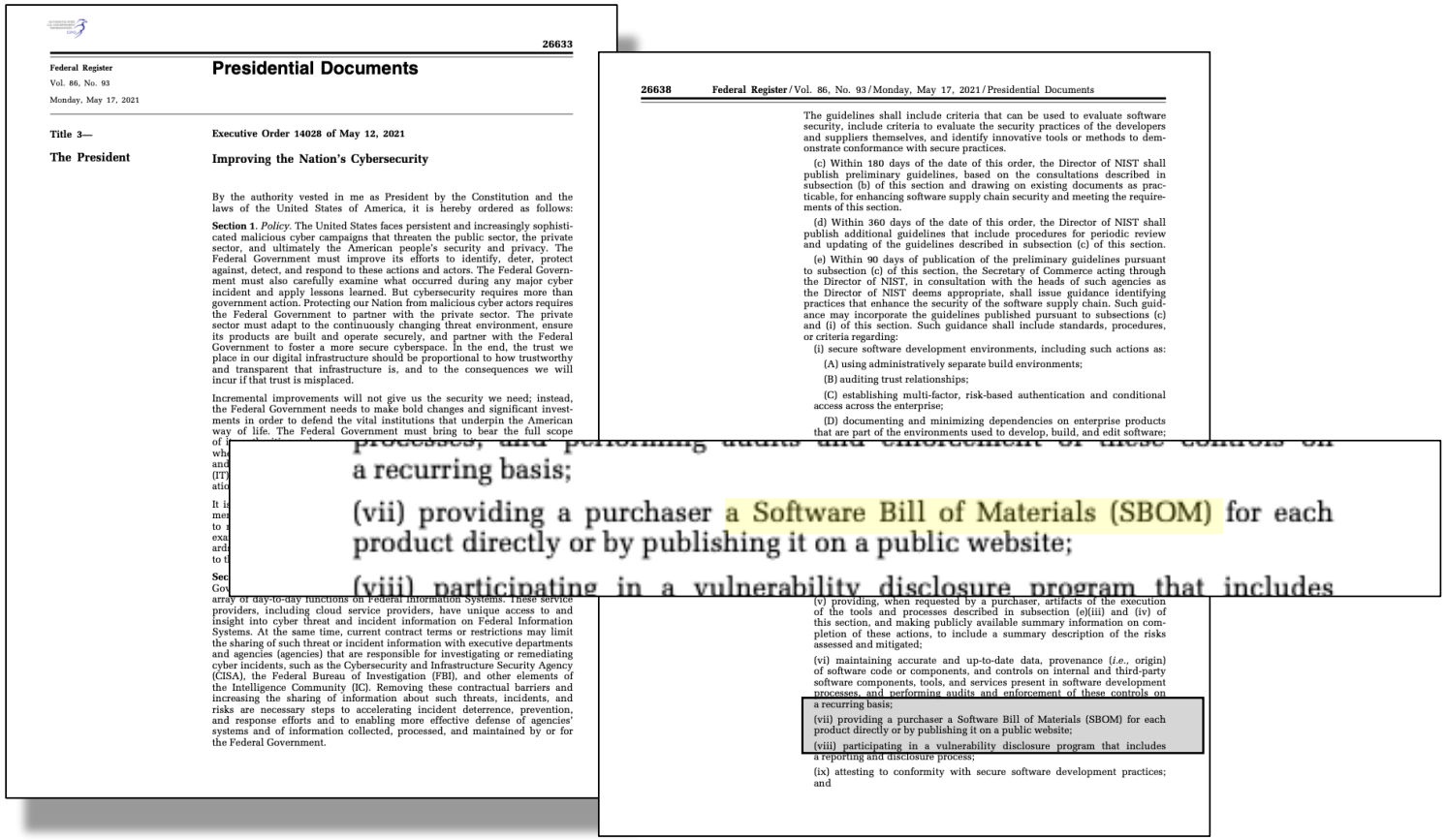
Subscribe to the SecurityWeek Email Briefing to stay informed on the latest threats, trends, and technology, along with insightful columns from industry experts.

Business Email Address...

Subscribe

Webinar: How to Build Resilience Against Emerging Cyber Threats

What is driving adoption of SBOMs?
May 2021 - Executive Order 14028 – “Improving the Nation’s Cybersecurity”



26633

Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

Title 3—
The President

Executive Order 14028 of May 12, 2021

Improving the Nation’s Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy*. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of i
who
and
(IT)
atio

It is
mea
to r
exa
ard
to t

Sec
Gov
array of day-to-day functions on Federal information Systems. These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence Community (IC). Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies’ systems and of information collected, processed, and maintained by or for the Federal Government.

26638 Federal Register / Vol. 86, No. 93 / Monday, May 17, 2021 / Presidential Documents

The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.

(c) Within 180 days of the date of this order, the Director of NIST shall publish preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section.

(d) Within 360 days of the date of this order, the Director of NIST shall publish additional guidelines that include procedures for periodic review and updating of the guidelines described in subsection (c) of this section.

(e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section. Such guidance shall include standards, procedures, or criteria regarding:

(i) secure software development environments, including such actions as:

(A) using administratively separate build environments;

(B) auditing trust relationships;

(C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;

(D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;

a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes

(v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;

(vi) maintaining accurate and up-to-date data, provenance (*i.e.*, origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices; and

What Can and Can't SBOMs Do?

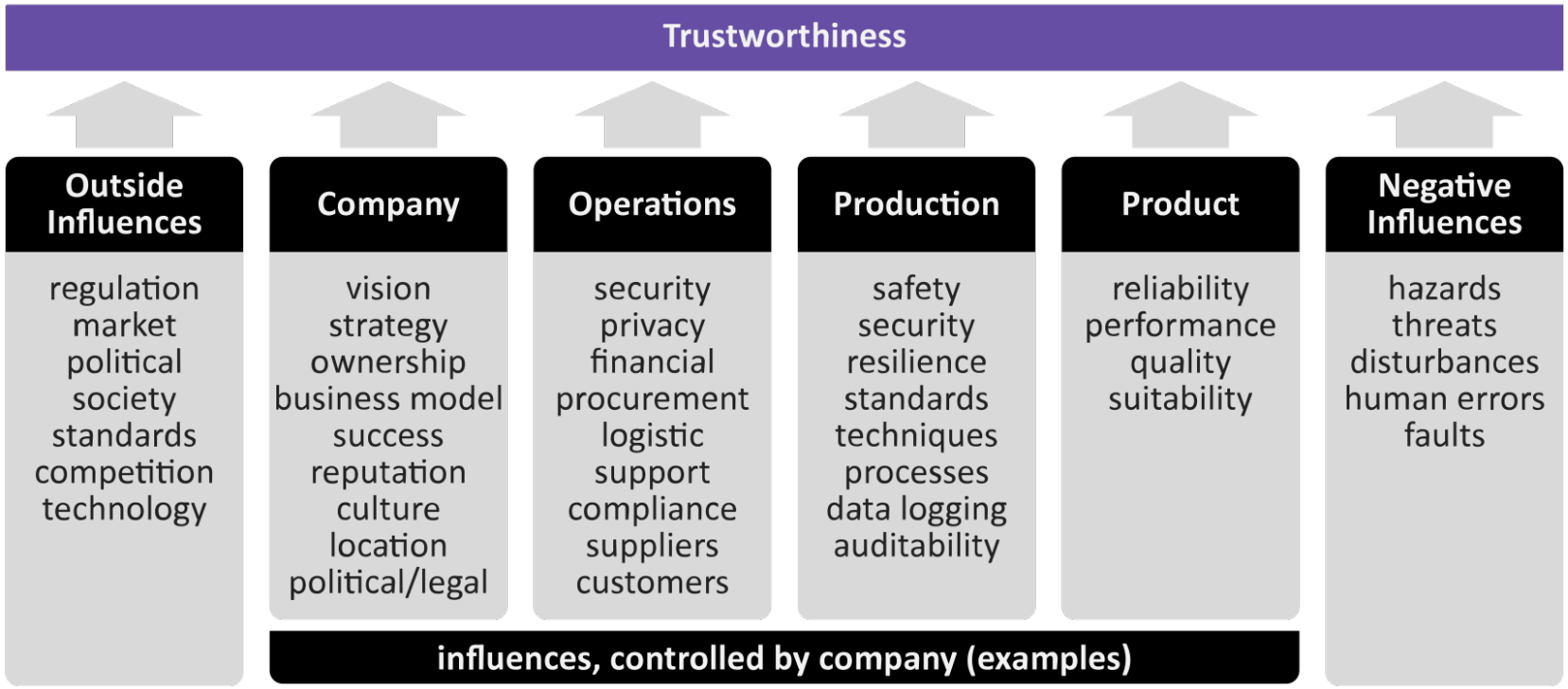
SBOMs CAN:

- 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:

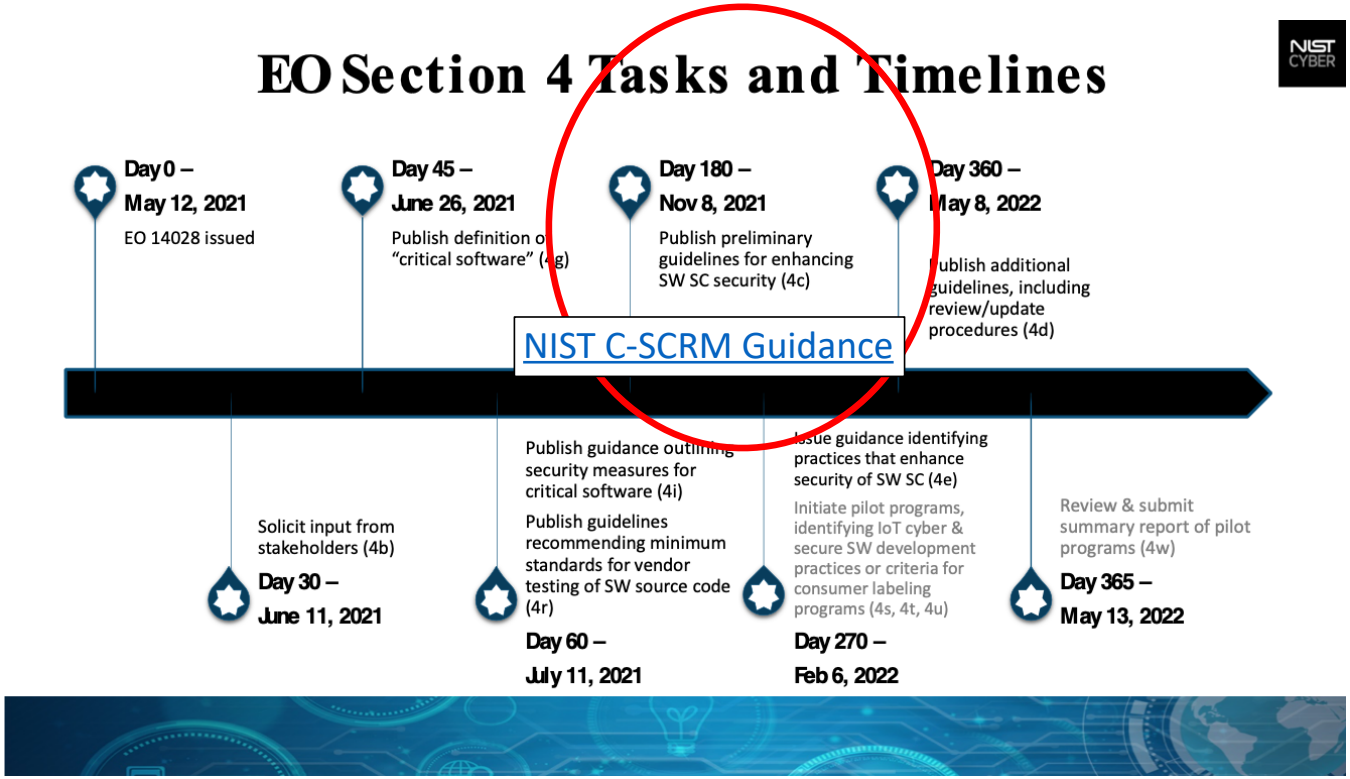
- Provide protection without other tools or interventions
- Replace EDR, SoC, or other security measures
- Be a source of threat intelligence before a vulnerability is revealed

What Makes a Trusted Partner?

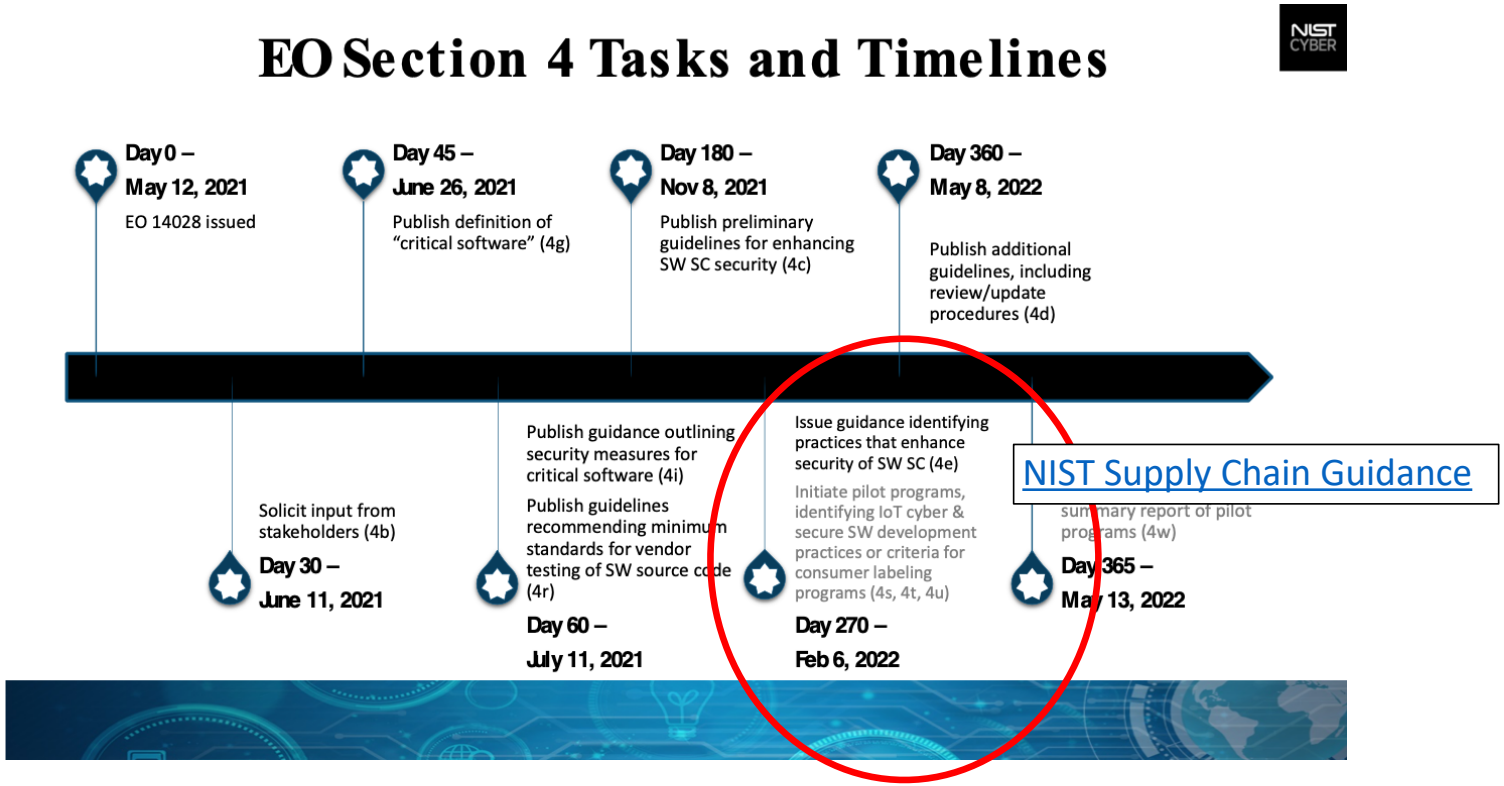


From Industrial Internet Consortium: “Trustworthiness Framework Foundations,” 2021-05-27

NIST C-SCRM – Executive Order 14028 – "Software Supply Chain Security"



NIST SSDF – Executive Order 14028 – ” Consumer Labeling”



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

Verbatim from Labeling Doc: February 4, 2022

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 underltying components, dealing with pre- and post-EOL vulns/defects)

Verbatim from Labeling Doc: February 4, 2022

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, E maintenance, breach disclosure and mitigation)

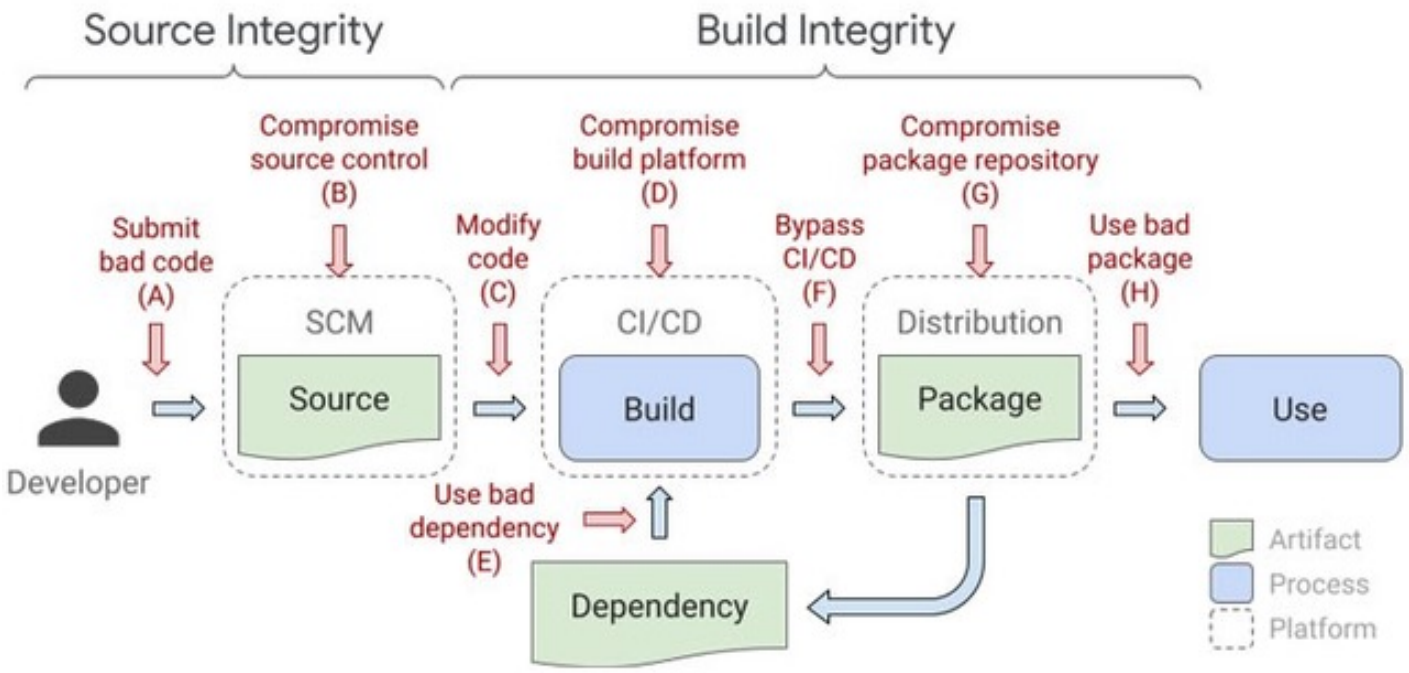
Product Education and Awareness (cybersec capability/instructions)

SBOM

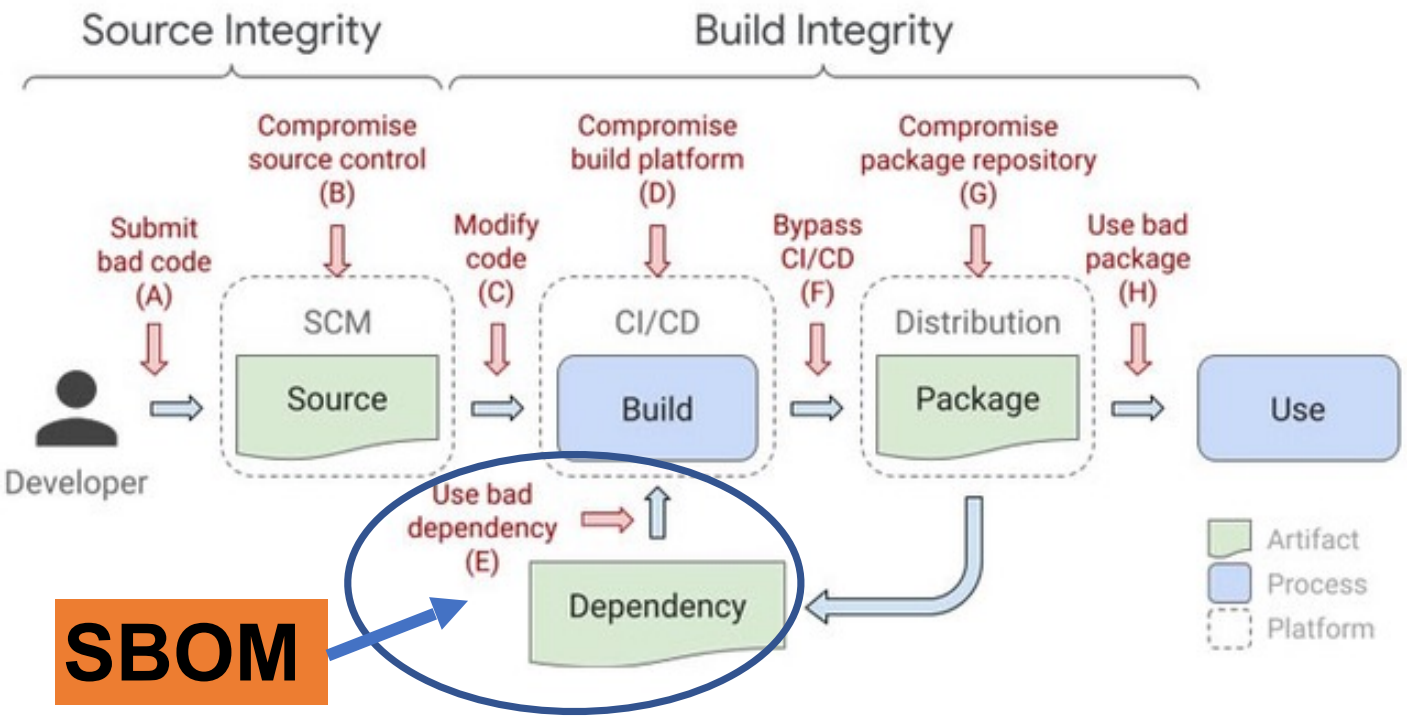
Documentation

- 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 underltying components, dealing with pre- and post-EOL vulns/defects)

Supply Chain Levels for Software Artifacts (SLSA) - Basic Map of SDLC



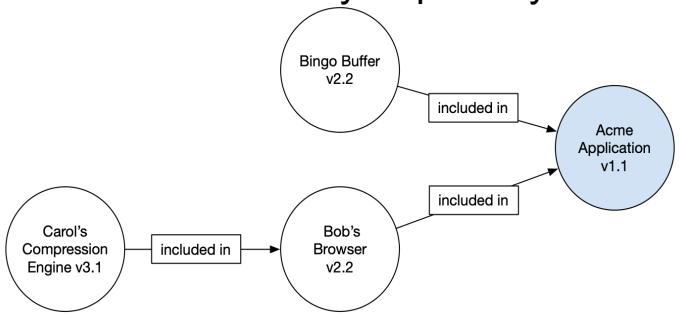
SLSA – Basic Map



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



Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Self
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

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

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

Cyclone DX (XML): Cisco AMP/Android

```
<?xml version="1.0"?>
<bom serialNumber="urn:uuid:1ecf1de9-3bad-8cbd-f451-053220fbbc0a"
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>
          <component type="device" bom-ref="24a36030-1f36-f9b7-e303-911ffd1756c3">
            <name>Cisco Secure Endpoints for Android</name>
            <version>2.1.0</version>
            <purl>pkg:supplier/Cisco/Cisco%20Secure%20Endpoints%20for%20Android@2.1.
          </component>
          <manufacture>
            <name>Cisco</name>
            <url></url>
            <contact>
              <name>Cisco</name>
              <email></email>
            </contact>
          </manufacture>
          <supplier>
            <name>
              Cisco
            </name>
          </supplier>
        </metadata>
      <components>
        <component type="library" bom-ref="c639e5f9-557d-e679-1a76-5f70c146fea1">
          <publisher>Square</publisher>
          <name>okhttp</name>
          <version> 4.2.2</version>
          <purl>pkg:supplier/Square/okhttp@ 4.2.2</purl>
        </component>
          <component type="library" bom-ref="81316144-6a5d-7c5d-fce5-d00d14a16a7c">
            <publisher>design</publisher>
            <name>design </name>
            <version>2.0.3</version>
            <purl>pkg:supplier/design/design%20@2.0.3</purl>
          </component>
          <component type="library" bom-ref="d64804d5-18e5-24e8-89c3-7b886fad47d3">
            <publisher>Bouncy Castle</publisher>
            <name>bouncy-castle</name>
            <version>1.62.0</version>
            <purl>pkg:supplier/Bouncy%20Castle/bouncy-castle@1.62.0</purl>
          </component>
          <component type="library" bom-ref="ad911248-0914-a295-ed08-30de80fe87af">
            <publisher>Apache Santuario</publisher>
            <name>xmlsec-java</name>
            <version>2.1.4</version>
            <purl>pkg:supplier/Apache%20Santuario/xmlsec-java@2.1.4</purl>
          </component>
        </components>
<dependencies>
<dependency ref="24a36030-1f36-f9b7-e303-911ffd1756c3">
  <dependency ref="c639e5f9-557d-e679-1a76-5f70c146fea1"/>
  <dependency ref="81316144-6a5d-7c5d-fce5-d00d14a16a7c"/>
  <dependency ref="d64804d5-18e5-24e8-89c3-7b886fad47d3"/>
  <dependency ref="ad911248-0914-a295-ed08-30de80fe87af"/>
</dependency>
</dependencies>

</bom>
```

SBOM: Cisco AMP Endpoint for Android (CycloneDX format)

SPDX (Proprietary Format): Cisco AMP/Android (1/2)

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 DESCRIBES SPDXRef-Cisco-Secure-Endpoints-for-Android
Relationship: SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS NONE
PackageDownloadLocation: https://software.cisco.com/
FilesAnalyzed: true
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageHomePage: https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html

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
Relationship: SPDXRef-okhttp CONTAINS NOASSERTION
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: <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-
Relationship: SPDXRef-design- CONTAINS NOASSERTION
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: true
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION

Continued next page…

NOTE: Not for official use – for illustration purposes only. Edited for brevity - Apache License text removed.

SPDX (Proprietary Format): Cisco AMP/Android (2/2)

```
## 2.4 All-Levels Components
##
PackageName: 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
## 2.4 All-Levels Components
##
PackageName: 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 version="1.0"?>
<bom serialNumber="urn:uuid:1ecf1de9-3bad-8cbd-f451-053220fbbc0a"
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>
      <component type="device" bom-ref="24a36030-1f36-f9b7-e303-911ffd1756c3">
        <name>Cisco Secure Endpoints for Android</name>
        <version>2.1.0</version>
        <purl>pkg:supplier/Cisco/Cisco%20Secure%20Endpoints%20for%20Android@2.1.
      </component>
      <manufacture>
        <name>Cisco</name>
        <url></url>
        <contact>
          <name>Cisco</name>
          <email></email>
        </contact>
      </manufacture>
      <supplier>
        <name>
          Cisco
        </name>
      </supplier>
    </metadata>
  <components>
    <component type="library" bom-ref="c639e5f9-557d-e679-1a76-5f70c146fea1">
      <publisher>Square</publisher>
      <name>okhttp</name>
      <version> 4.2.2</version>
      <purl>pkg:supplier/Square/okhttp@ 4.2.2</purl>
    </component>
```

```
    <component type="library"                                    0d14a16a7c">
      <publisher>design</publ
      <name>design </name>
      <version>2.0.3</versio
      <purl>pkg:supplier/desi
    </component>
    <component type="library"                                    886fad47d3">
      <publisher>Bouncy Castl
      <name>bouncy-castle</n
      <version>1.62.0</
      <purl>pk                                                   rl>
    </
                                                                 de80fe87af">
      <publisher>Apache Santu
      <name>xmlsec-java</name
      <version>2.1.4</versio
      <purl>pkg:supplier/Apache%20Santuario/xmlsec-java@2.1.4</purl>
    </component>
  </components>
<dependencies>
<dependency ref="24a36030-1f36-f9b7-e303-911ffd1756c3">
  <dependency ref="c639e5f9-557d-e679-1a76-5f70c146fea1"/>
  <dependency ref="81316144-6a5d-7c5d-fce5-d00d14a16a7c"/>
  <dependency ref="d64804d5-18e5-24e8-89c3-7b886fad47d3"/>
  <dependency ref="ad911248-0914-a295-ed08-30de80fe87af"/>
</dependency>
</dependencies>

</bom>
```

SBOM Header Fields

SBOM: Cisco AMP Endpoint for Android (CycloneDX format)

Cyclone DX (XML): Cisco AMP/Android


```
<?xml version="1.0"?>
<bom serialNumber="urn:uuid:1e
version = "1" xmlns="http://cy
        <metadata>
          <timestamp>2021-06-1
          <authors>
            <author>
              <name>Omar Santo
              <email></email>
            </author>
          </authors>
          <component type="dev
            <name>Cisco Secure
            <version>2.1.0</ve
            <purl>pkg:supplier
          </component>
          <manufacture>
            <name>Cisco</name>
            <url></url>
            <contact>
              <name>Cisco</nam
              <email></email>
            </contact>
          </manufacture>
          <supplier>
            <name>
              Cisco
            </name>
          </supplier>
        </metadata>
      <components>
        <component type="library" bom-ref="c639e5f9-557d-e679-1a76-5f70c146fea1">
          <publisher>Square</publisher>
          <name>okhttp</name>
          <version> 4.2.2</version>
          <purl>pkg:supplier/Square/okhttp@ 4.2.2</purl>
        </component>
```

```
11ffd1756c3">

%20Android@2.1.
```

```
        <component type="library" bom-ref="81316144-6a5d-7c5d-fce5-d00d14a16a7c">
          <publisher>design</publisher>
          <name>design </name>
          <version>2.0.3</version>
          <purl>pkg:supplier/design/design%20@2.0.3</purl>
        </component>
        <component type="library" bom-ref="d64804d5-18e5-24e8-89c3-7b886fad47d3">
          <publisher>Bouncy Castle</publisher>
          <name>bouncy-castle</name>
          <version>1.62.0</version>
          <purl>pkg:supplier/Bouncy%20Castle/bouncy-castle@1.62.0</purl>
        </component>
        <component type="library" bom-ref="ad911248-0914-a295-ed08-30de80fe87af">
          <publisher>Apache Santuario</publisher>
          <name>xmlsec-java</name>
          <version>2.1.4</version>
          <purl>pkg:supplier/Apache%20Santuario/xmlsec-java@2.1.4</purl>
        </component>
      </components>
<dependencies>
<dependency ref="24a36030-1f36-f9b7-e303-911ffd1756c3">
  <dependency ref="c639e5f9-557d-e679-1a76-5f70c146fea1"/>
  <dependency ref="81316144-6a5d-7c5d-fce5-d00d14a16a7c"/>
  <dependency ref="d64804d5-18e5-24e8-89c3-7b886fad47d3"/>
  <dependency ref="ad911248-0914-a295-ed08-30de80fe87af"/>
</dependency>
</dependencies>

</bom>
```

SBOM: Cisco AMP Endpoint for Android (CycloneDX format)

Cyclone DX (XML): Cisco AMP/Android

```
<?xml version="1.0"?>
<bom serialNumber="urn:uuid:1ecf1de9-3bad-8cbd-f451-053220fbbc0a"
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>
          <component type="device" bom-ref="24a36030-1f36-f9b7-e303-911ffd1756c3">
            <name>Cisco Secure Endpoints for Android</name>
            <version>2.1.0</version>
            <purl>pkg:supplier/Cisco/Cisco%20Secure%20Endpoints%20for%20Android@2.1.
          </component>
          <manufacture>
            <name>Cisco</name>
            <url></url>
            <contact>
              <name>Cisco</name>
              <email></email>
            </contact>
          </manufacture>
          <supplier>
            <name>
              Cisco
            </name>
          </supplier>
        </metadata>
      <components>
        <component type="library" bom-ref="c639e5f9-557d-e679-1a76-5f70c146fea1">
          <publisher>Square</publisher>
          <name>okhttp</name>
          <version> 4.2.2</version>
          <purl>pkg:supplier/Square/okhttp@ 4.2.2</purl>
        </component>
```

Component Dependencies (i.e. Relationships)

```
          <component type="library" bom-ref="81316144-6a5d-7c5d-fce5-d00d14a16a7c">
            <publisher>design</publisher>
            <name>design </name>
            <version>2.0.3</version>
            <purl>pkg:supplier/design/design%20@2.0.3</purl>
          </component>
          <component type="library" bom-ref="d64804d5-18e5-24e8-89c3-7b886fad47d3">
            <publisher>Bouncy Castle</publisher>
            <name>bouncy-castle</name>
            <version>1.62.0</version>
            <purl>pkg:supplier/Bouncy%20Castle/bouncy-castle@1.62.0</purl>
          </component>
          <component type="library" bom-ref="ad911248-0914-a295-ed08-30de80fe87af">
            <publisher>Apache Santuario</publisher>
            <name>xmlsec-java</name>
            <version>2.1.4</version>
            <purl>pkg:supplier/Apache%20Santuario/xmlsec-java@2.1.4</purl>
          </component>
        </components>
<dependencies>
<dependency ref="24a36030-1f36-f9b7-e303-911ffd1756c3">
  <dependency ref="c639e5f9-557d-e679-1a76-5f70c146fea1"/>
  <dependency ref="81316144-6a5d-7c5d-fce5-d00d14a16a7c"/>
  <dependency ref="d64804d5-18e5-24e8-89c3-7b886fad47d3"/>
  <dependency ref="ad911248-0914-a295-ed08-30de80fe87af"/>
</dependency>
</dependencies>

</bom>
```

SBOM: Cisco AMP Endpoint for Android (CycloneDX format)

SPDX (Proprietary Format): Cisco AMP/Android (1/2)

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 DESCRIBES SPDXRef-Cisco-Secure-Endpoints-for-Android
Relationship: SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS NONE
PackageDownloadLocation: https://software.cisco.com/
FilesAnalyzed: true
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageHomePage: https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html

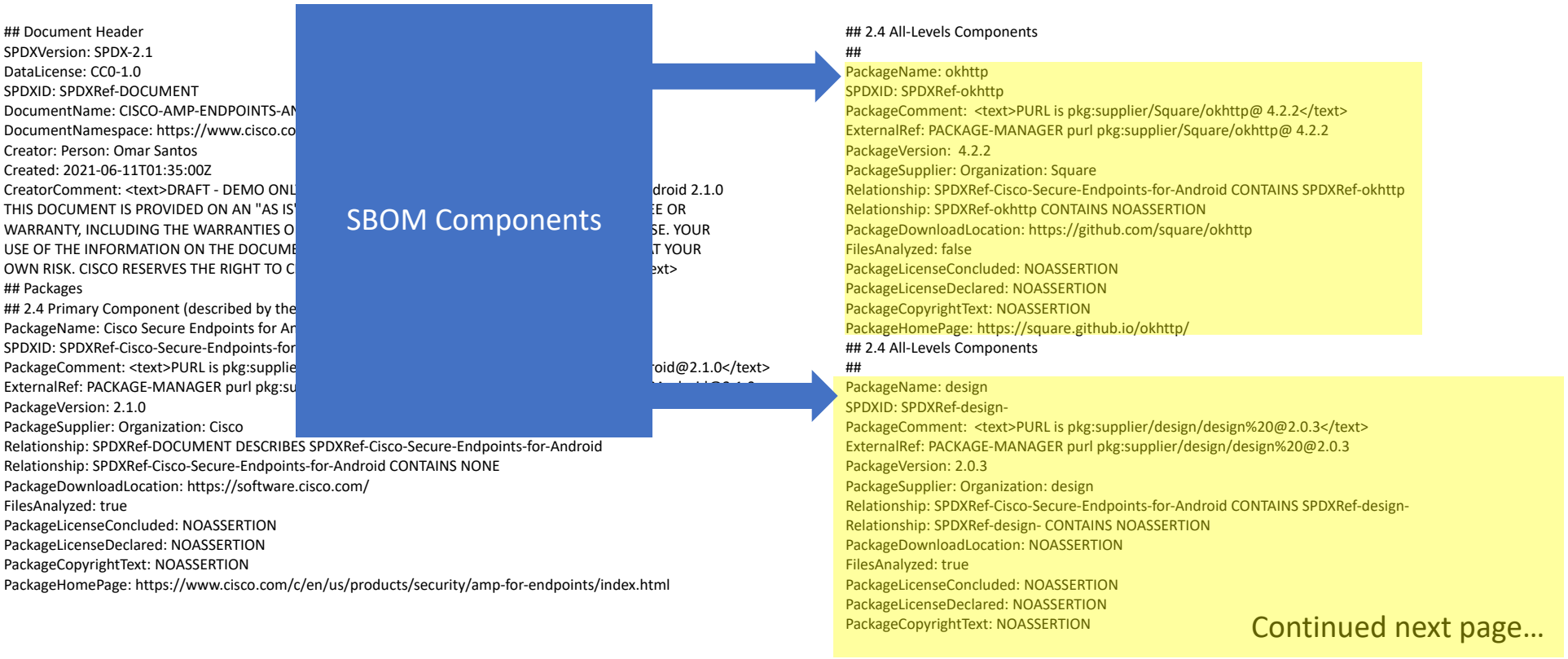
SBOM Header Fields

2.4 All-Levels Components
##
PackageName: okhttp
SPDXID: SPDXRef-okhttp
PackageComment: <text>PURL is pkg:sup
ExternalRef: PACKAGE-MANAGER purl pk
PackageVersion: 4.2.2
PackageSupplier: Organization: Square
Relationship: SPDXRef-Cisco-Secure-Endp
Relationship: SPDXRef-okhttp CONTAINS
PackageDownloadLocation: htt
FilesAnalyzed: false
Package
PackageCopyrightText: NOASSERTION
PackageHomePage: https://square.github
2.4 All-Levels Components
##
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-
Relationship: SPDXRef-design- CONTAINS NOASSERTION
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: true
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION

Continued next page…

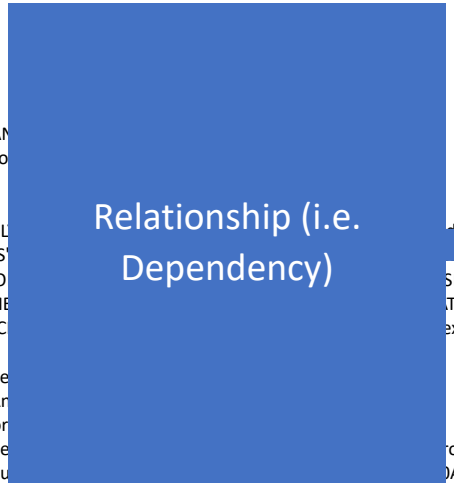
NOTE: Not for official use – for illustration purposes only. Edited for brevity - Apache License text removed.

SPDX (Proprietary Format): Cisco AMP/Android (1/2)



NOTE: Not for official use – for illustration purposes only. Edited for brevity - Apache License text removed.

SPDX (Proprietary Format): Cisco AMP/Android (1/2)



Document Header
SPDXVersion: SPDX-2.1
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: CISCO-AMP-ENDPOINTS-AN
DocumentNamespace: https://www.cisco.co
Creator: Person: Omar Santos
Created: 2021-06-11T01:35:00Z
CreatorComment: <text>DRAFT - DEMO ONL
THIS DOCUMENT IS PROVIDED ON AN "AS IS"
WARRANTY, INCLUDING THE WARRANTIES O
USE OF THE INFORMATION ON THE DOCUME
OWN RISK. CISCO RESERVES THE RIGHT TO C
Packages
2.4 Primary Component (described by the
PackageName: Cisco Secure Endpoints for An
SPDXID: SPDXRef-Cisco-Secure-Endpoints-for
PackageComment: <text>PURL is pkg:supplie
ExternalRef: PACKAGE-MANAGER purl pkg:su
PackageVersion: 2.1.0
PackageSupplier: Organization: Cisco
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Cisco-Secure-Endpoints-for-Android
Relationship: SPDXRef-Cisco-Secure-Endpoints-for-Android CONTAINS NONE
PackageDownloadLocation: https://software.cisco.com/
FilesAnalyzed: true
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageHomePage: https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html

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
Relationship: SPDXRef-okhttp CONTAINS NOASSERTION
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: <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-
Relationship: SPDXRef-design- CONTAINS NOASSERTION
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: true
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION

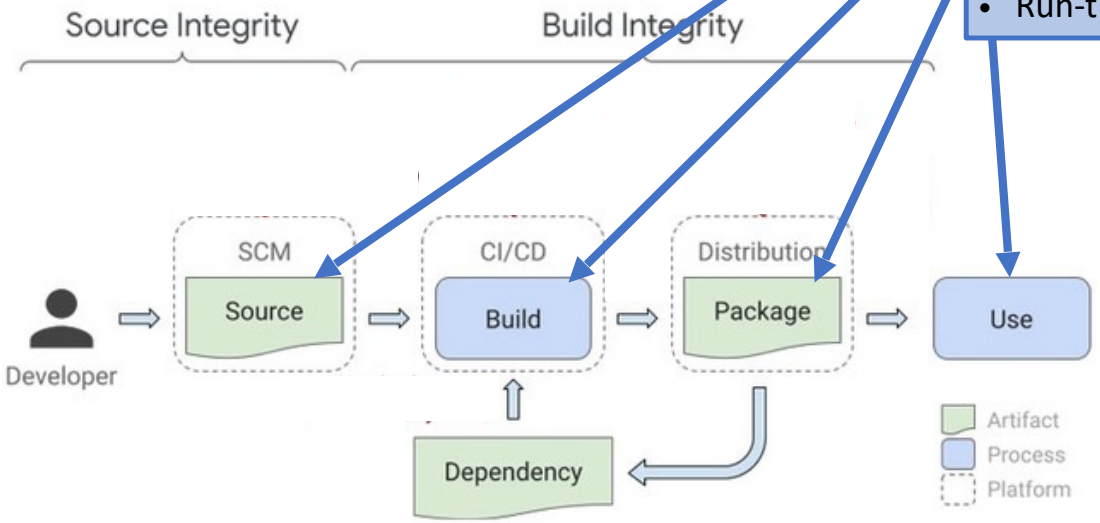
Continued next page…

NOTE: Not for official use – for illustration purposes only. Edited for brevity - Apache License text removed.

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

Phase 1 Output – July 2019
13 Automotive Concerns for NTIA

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
- DBOM - decentralized approach to sharing with a policy base
- Trust Store (Hitachi)
- Email, ftp,
- Software installation kits
- Industry/vendor/supplier portals
- TAXII https://oasis-open.github.io/cti-documentation/taxii/intro.html (?)
- Manufacturer Disclosure Statement for Medical (MDS2) form (2019)
  - https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security
- ISAC e.g. https://h-isac.org/tag/sbom/
- MISP Threat Sharing https://www.misp-project.org/
- OpenC2
- Commercial products - cybersecurity, supply chain, secure document exchange
- **OTA??**

Thank you! Questions?