Software Bill of Materials In The Automotive Industry

Charlie Hart
Hitachi America Ltd –Research and Development Group

March 24, 2022

About the Speaker

HITACHI
Inspire the Next

Charlie Hart
Hitachi America Ltd.

Current Positions

- Senior Analyst, Security, Hitachi America R&D
- Chairman, Automotive ISAC Supplier Affinity Group SBOM Working Group

Past Positions

- Senior Vice President, Software and Solutions Engineering, Hitachi Data Systems
- Vice President, OSS Engineering, Savvis
- Senior Director, Software Engineering, Sun Microsystems
- Vice President, Software Infrastructure Engineering, Veritas Software
- Vice President, Systems Security/Services Engineering, StorageNetworks
- Vice President, Technology Systems and Services, Massachusetts Financial Services
- Project Specialist/Programmer Analyst, Software Services, Digital Equipment Corporation

Education

- Bachelor of Arts, English – Boston College

Agenda

HITACHI
Inspire the Next

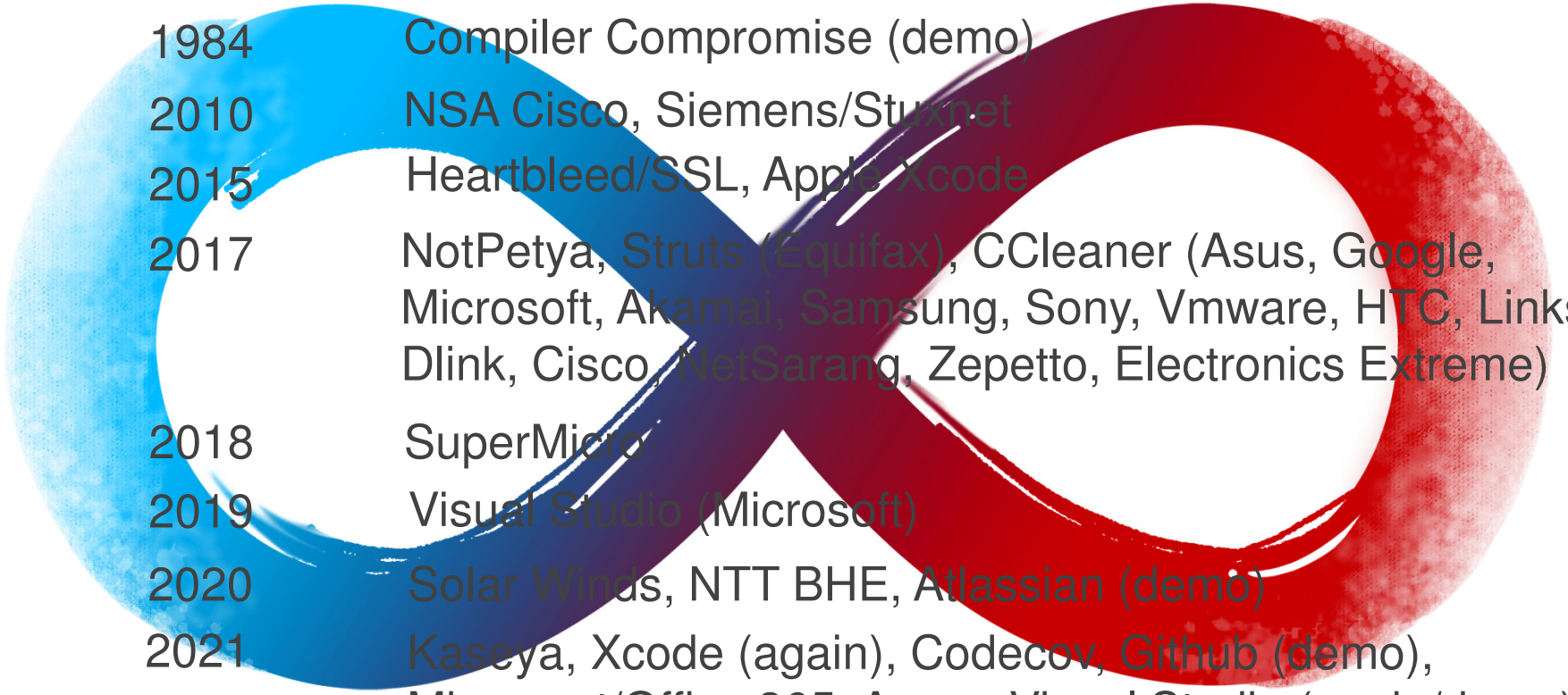
- Why SBOM Matters to the Automotive Industry
- Automotive ISAC and SBOM – History, Details, and Status
- Next Steps

HITACHI
Inspire the Next

Why SBOM Matters to the Automotive Industry

Software Supply Chain Attacks – A Brief History

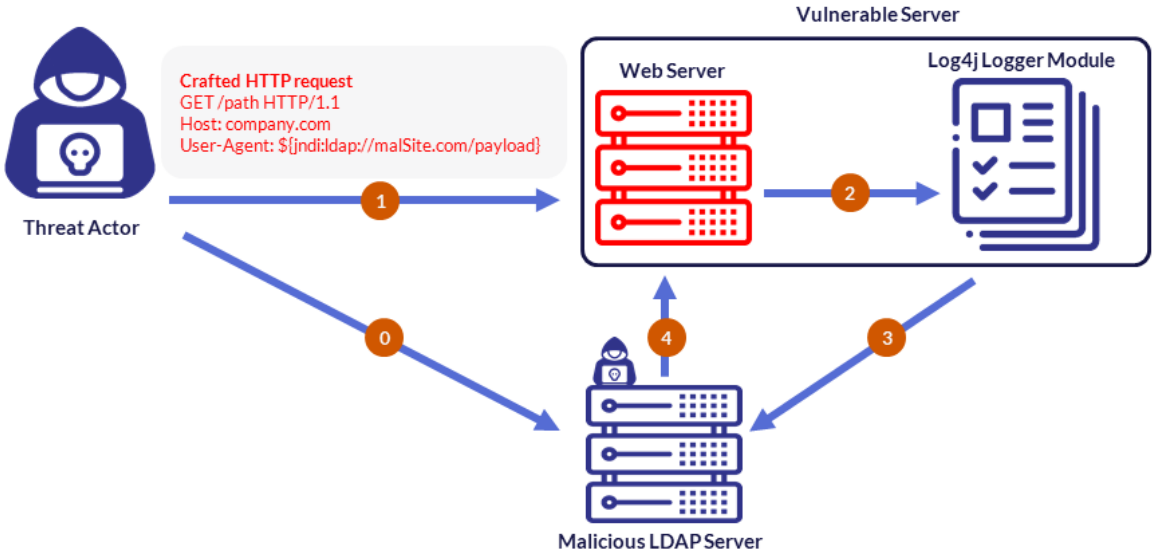
HITACHI
Inspire the Next



1984	Compiler Compromise (demo)
2010	NSA Cisco, Siemens/Stuxnet
2015	Heartbleed/SSL, Apple Xcode
2017	NotPetya, Struts (Equifax), CCleaner (Asus, Google, Microsoft, Akamai, Samsung, Sony, Vmware, HTC, Linksys, Dlink, Cisco, NetSarang, Zepetto, Electronics Extreme)
2018	SuperMicro
2019	Visual Studio (Microsoft)
2020	Solar Winds, NTT BHE, Atlassian (demo)
2021	Kaseya, Xcode (again), Codecov, Github (demo), Mimecast/Office 365, Azure, Visual Studio (again/demo), Compiler Compromise (demo)

Log4j

HITACHI
Inspire the Next



0. Threat actor setting up his malicious LDAP server with malicious Java class
1. Threat actor sends malicious payload that is likely to be logged by the application
2. Payload passed to Log4j for logging
3. Log4j parse the payload and make a query to the malicious LDAP server
4. The LDAP server responds with content that holds the malicious java class

NHTSA – “Cybersecurity Best Practices for the Safety of Modern Vehicles”

HITACHI
Inspire the Next

Cybersecurity Best Practices for the Safety of Modern Vehicles

Draft 2020 Update

U.S. Department of Transportation
National Highway Traffic Safety Administration

4.2.5 Protections

[G.8] For remaining functionality and underlying risks, layers of protection[17] that are appropriate for the assessed risks should be designed and implemented.

[G.9] Clear cybersecurity standards should be specified and communicated to the suppliers that support the intended protections.[18]

4.2.6 Inventory and Management of Software Assets on Vehicles

[G.10] Manufacturers should maintain a database of operational software components[19,20] used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime.

[G.11] Manufacturers should track sufficient details related to software components,[21] such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software,[22] manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.

4.2.7 Penetration Testing and Documentation

[G.12] Manufacturers should evaluate all commercial off-the-shelf and open-source software components used in vehicle ECUs against known vulnerabilities.[23,24]

[G.13] Manufacturers should also pursue product cybersecurity testing, including using

that support the intended protections.[18]

4.2.6 Inventory and Management of Software Assets on Vehicles

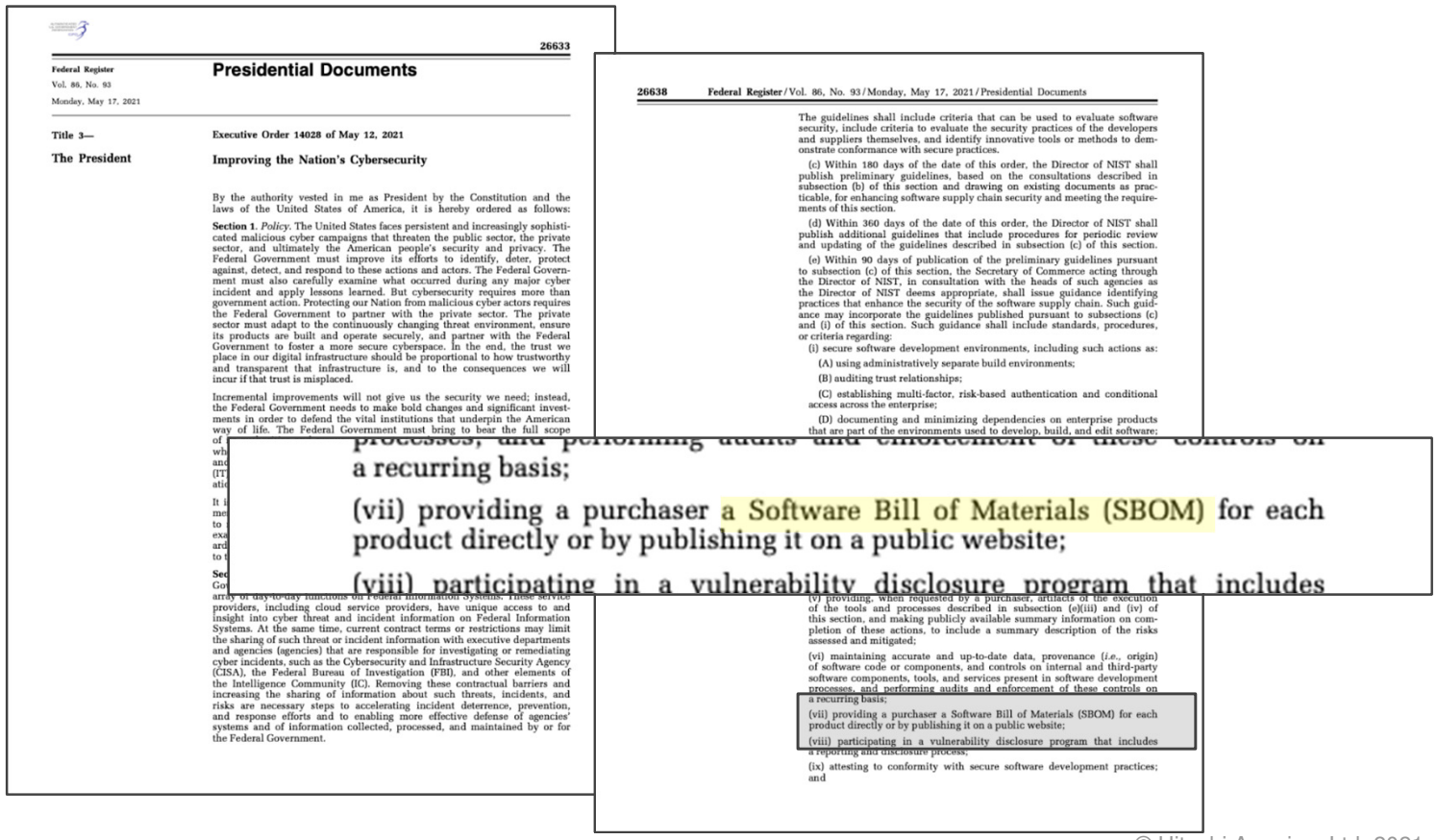
[G.10] Manufacturers should maintain a database of operational software components[19,20] used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime.

[G.11] Manufacturers should track sufficient details related to software components,[21] such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software,[22] manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.

4.2.7 Penetration Testing and Documentation

May 2021 - Executive Order 14028 – "Improving the Nation's Cybersecurity"

HITACHI
Inspire the Next



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

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

Major Regulation and Guidance

HITACHI
Inspire the Next

- **There are no current SBOM regulations in the auto industry.**
- But there is growing interest (e.g. NHTSA “Best Practice”)
- Note: Executive Order only applies to US Government purchases and operations – no force of law

Guidance from Governments

- **US** is the main global driver, influencing US allies and commercial vendors
  - DoC – **NTIA public/private multistakeholder program**, NIST guidance for USG and private industry
  - DHS – CISA - Next phase of SBOM guidance and regulation
  - DoE – SBOM PoC starting under the supervision of INL and PNNL
  - DoD – Long required for classified, recently expanded for unclassified, further expanded by EO 14028
  - FDA – Draft premarket guidance for medical devices issued
  - DoT - NHTSA – Cyber/safety best practices (expected to move from optional to required). DoT considering requiring for all federal vehicle purchases
  - EOP – NSC, OMB, others directing agency compliance with EO and other directives
- **Japan** METI and **EU** ENISA and others are considering guidance – likely similar to US

Guidance from Standards Bodies

- **ISO** – No requirements yet but requires risk analysis of code in 21434
- **UNECE WP.29** – No requirements yet but R155 requires demonstration of supplier-related risks

HITACHI
Inspire the Next

SBOMs and Automotive ISAC

Background – ISACs (Information Sharing and Analysis Centers)

HITACHI
Inspire the Next

- Post-9/11 concerns about systemic risk in US industry
- Presidential Policy Directive 21 directed DHS to foster public/private cooperation and coordination and listed the initial critical infrastructure sectors
- US Department of Homeland Security later designated 16 US critical infrastructure sectors specifically
- Automotive and related industries are designated part of the Critical Manufacturing sector (not specifically noted as a single sector)
- The legal advantage of ISACs is antitrust safe harbor. The biggest benefit is the community of industry and cybersecurity people.

FYI: “16” Critical Infrastructure Sectors

HITACHI
Inspire the Next

“There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”

https://www.cisa.gov/critical-infrastructure-sectors

- Chemicals
- Communications
- Dams
- Emergency Services
- Financial Services
- Government Facilities
- Information Technology
- Transportation Systems
- Commercial Facilities
- Critical Manufacturing
- Defense Industrial Base
- Energy
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Nuclear Reactors, Materials, and Waste
- Water and Wastewater Systems

AutoISAC SBOM Working Group - History

HITACHI
Inspire the Next

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 – Present

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 AWG SBOM SIG (Phase 1) – 2019
Goal: Members' Issues Addressed With NTIA

HITACHI
Inspire the Next

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?

Preview: Best Practice Guide Proposal

HITACHI
Inspire the Next

WILL INCLUDE

TLP AMBER 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

The Case Against SBOM – The Big Objections

HITACHI
Inspire the Next

1. **IP Concerns**
   - Licensing
   - Anticompetitive information
   - Violation of other contract terms
   - Unfair business or negotiating advantage to consumer
2. **Legal, Liability, and Regulatory Concerns**
3. **Making Hacking Easy**

All were reconciled (or nearly so) with members' concerns in the Best Practice Guide Draft

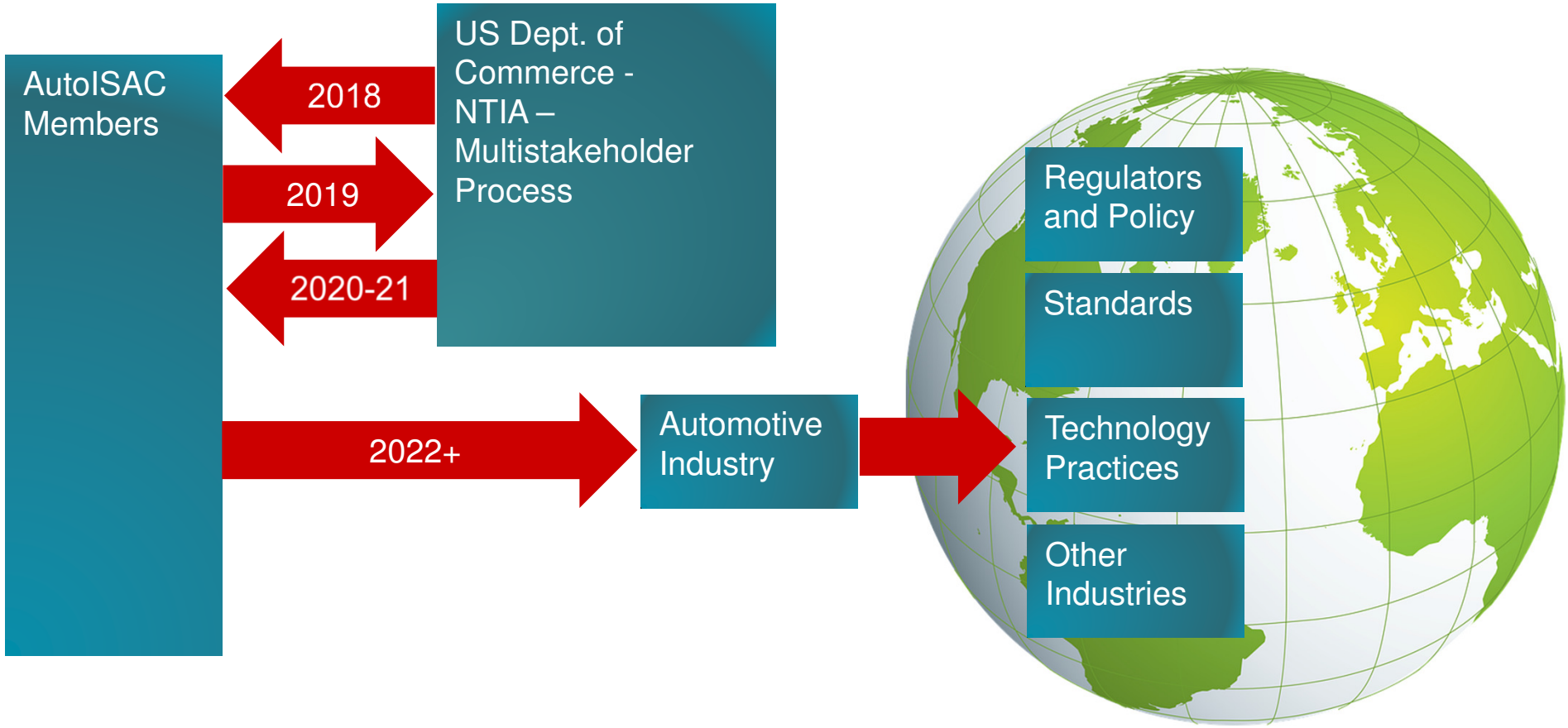
Next Steps

HITACHI
Inspire the Next

1. **Finalize Best Practice Draft Proposal (Done)**
2. **Board of Directors approval**
3. **Phase 3 (Likely)– active exercise – details under discussion**
4. **Future Possibilities (not decided)**
    - Limited production pilot exercise
    - Training program
    - Automation and tool trials
    - DHS/CISA program (NTIA successor)
    - Supply chain integrity exercise
    - Vulnerability management use case and exercise
    - Addition of Vulnerability/Exploitability eXchange (VEX) automation

Cooperation, Education, and Guidance

HITACHI
Inspire the Next



HITACHI

Inspire the Next

HITACHI
Inspire the Next

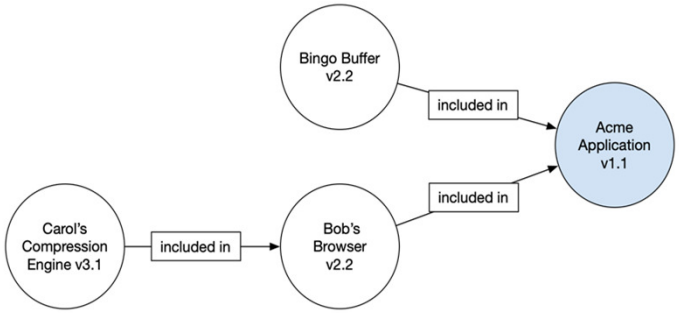
Introduction – Software Bill of Materials

Software Bill of Materials (SBOM)

HITACHI
Inspire the Next

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 Best 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 - “Minimum Viable Product”

HITACHI
Inspire the Next

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	Cryptographic code check to ensure component matches SBOM references
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.

What Formats Are Used For Specifying SBOMs?

HITACHI
Inspire the Next

- **SPDX – Software Package Data Exchange https://spdx.dev**
  - Linux Foundation-sponsored
  - Originally intended for open source license catalog
  - Robust support
  - Purpose-built adaptation for SBOM by Linux Foundation
- **SWID – SoftWare IDentification (tag) https://csrc.nist.gov/projects/Software-Identification-SWID**
  - ISO/IEC 19770-2
  - Intended for inventory tracking, works for SBOM also
  - NIST support, full info requires ISO or IEC subscription
  - Software attribute tagging
- **CycloneDX - https://cyclonedx.org**
  - OWASP CycloneDX Core Working Group
  - Extensions available for programming environments
  - Native extended (i.e superset of the NTIA guidance) SBOM support
  - Good support, newer to program but highly developed