SBOMs in the Automotive Industry – Auto-ISAC SBOM Working Group

Charlie Hart

Senior Analyst, Hitachi America R&D

Chair, Automotive ISAC SBOM Working Group

SBOM-a-rama - June 14, 2023

The Next 10 Minutes

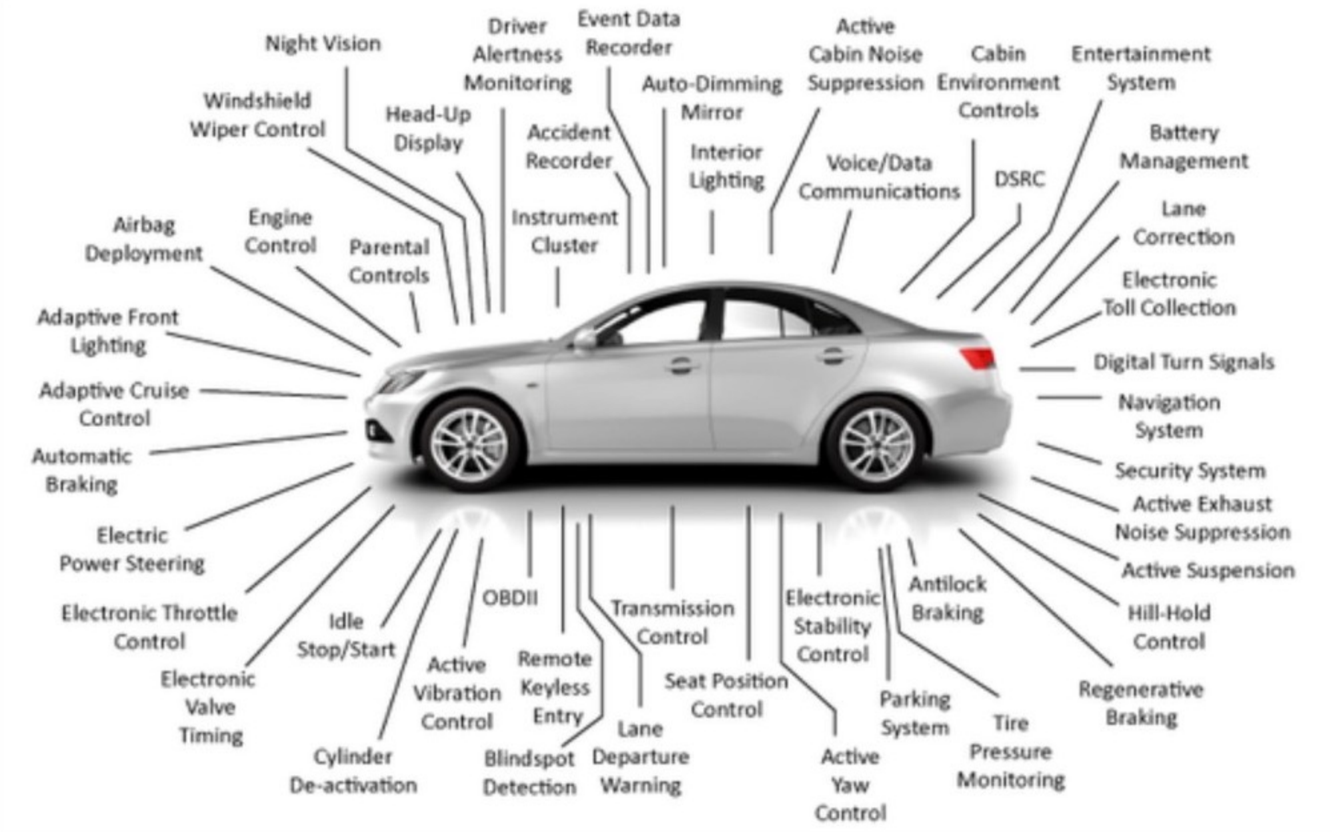
- Background on the automotive industry
- Cybersecurity and Cars
- Auto-ISAC SBOM Working Group
- Phase 3 – latest status

(Thanks to Alison Hwang from Auto-ISAC!)

The Automotive Industry

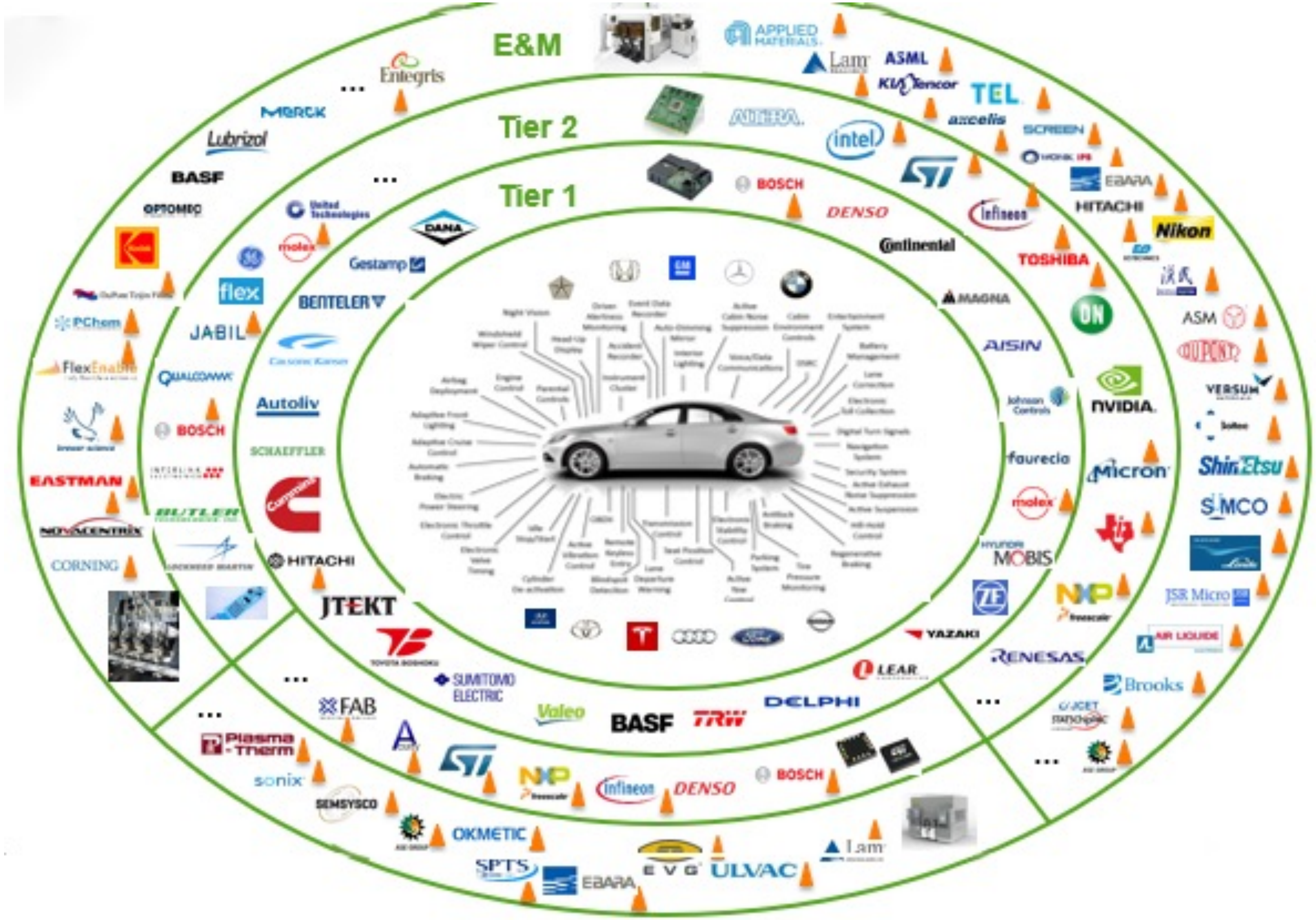
- $3+ trillion
- 50 countries
- 1000s of suppliers
- ~60 million vehicles built/year
- Highly regulated – global, national, state/province
- 30,000 parts/car
- Safety of road users is THE priority

Cybersecurity and Cars

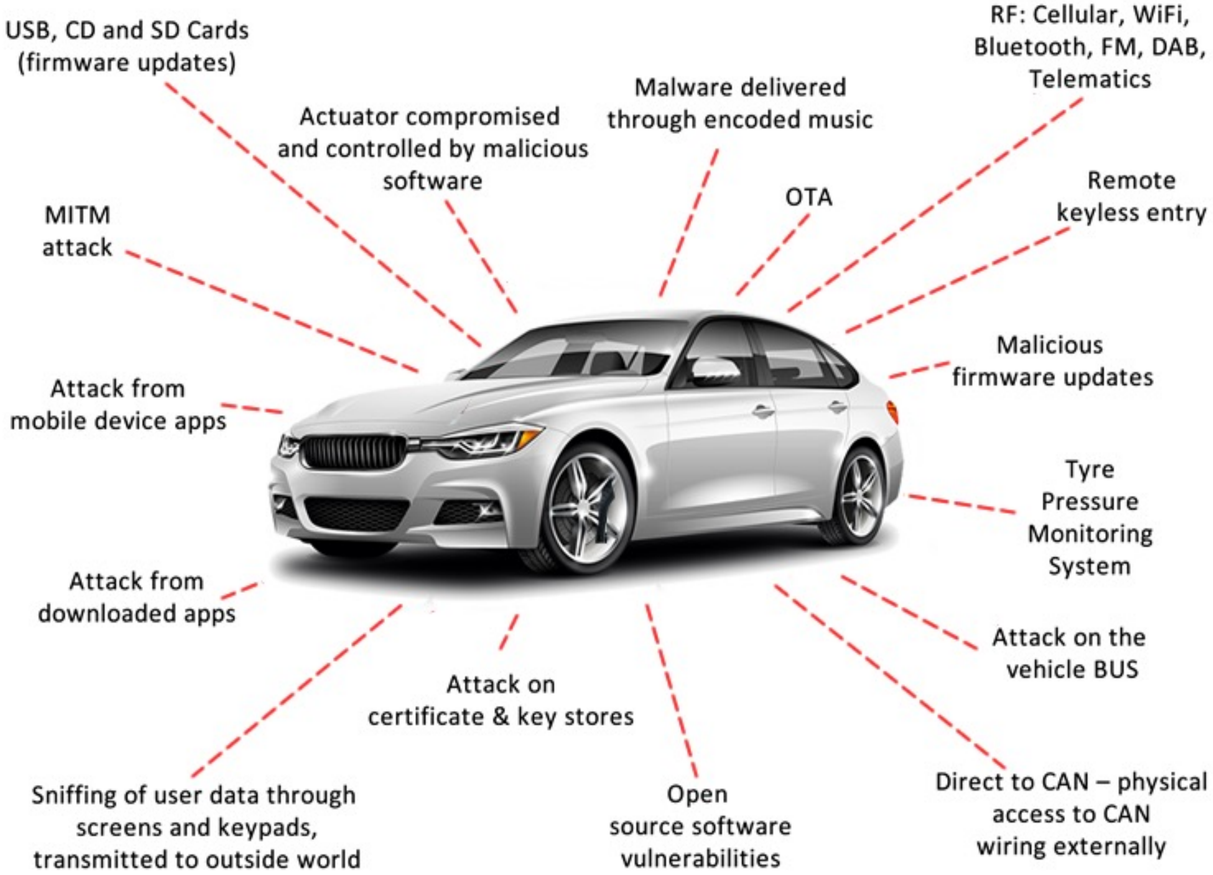


"The car is a computer."

Cybersecurity and Cars – Supply Chain

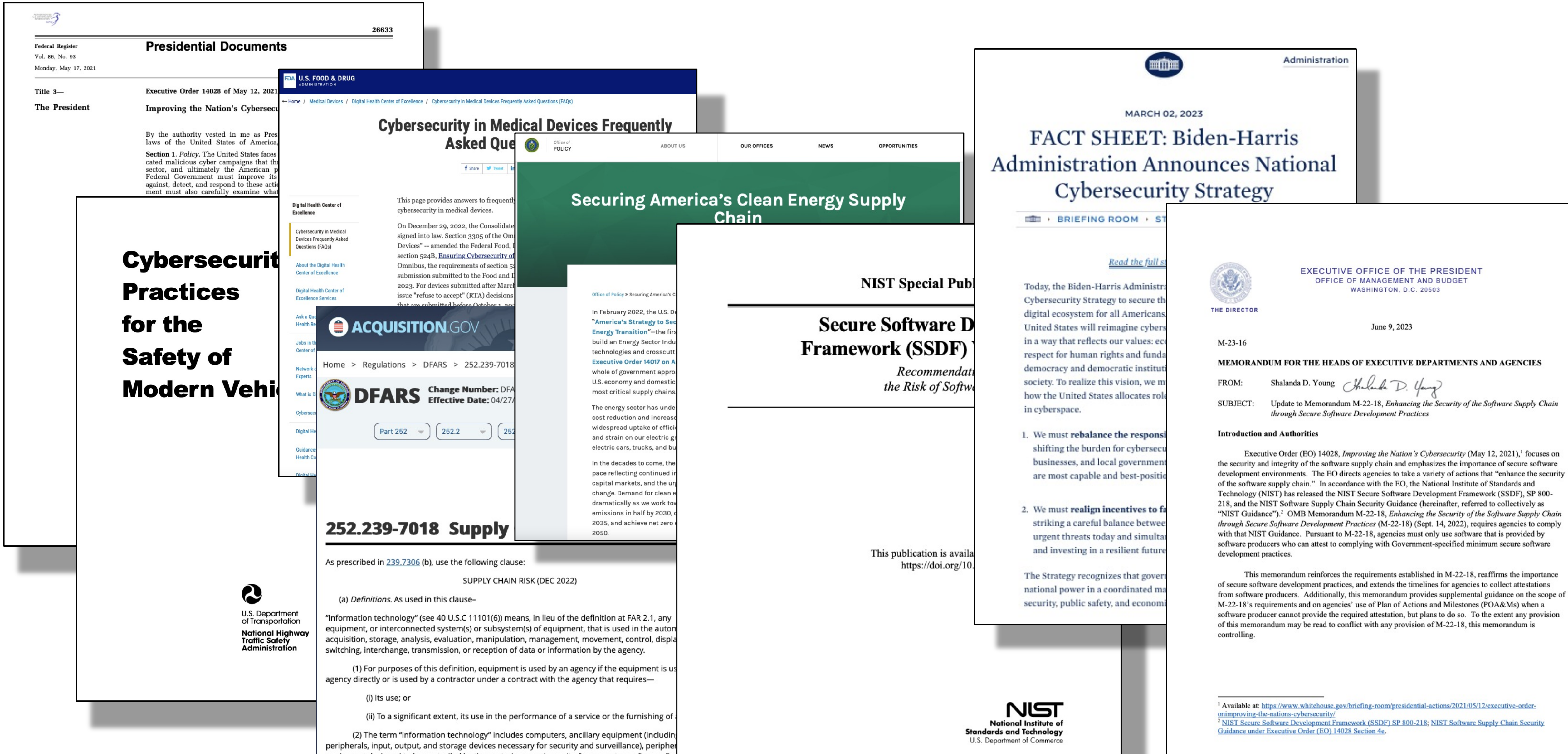


Cybersecurity in Cars – Attack Vectors and Consequences



USB, CD and SD Cards (firmware updates)
Actuator compromised and controlled by malicious software
Malware delivered through encoded music
RF: Cellular, WiFi, Bluetooth, FM, DAB, Telematics
MITM attack
OTA
Remote keyless entry
Malicious firmware updates
Attack from mobile device apps
Tyre Pressure Monitoring System
Attack from downloaded apps
Attack on the vehicle BUS
Attack on certificate & key stores
Sniffing of user data through screens and keypads, transmitted to outside world
Open source software vulnerabilities
Direct to CAN – physical access to CAN wiring externally

SBOM: A Flurry of Regulations and Guidance



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 Cybersecu

By the authority vested in me as Pres
laws of the United States of America,

Section 1. *Policy*. The United States faces
cated malicious cyber campaigns that thr
sector, and ultimately the American p
Federal Government must improve its
against, detect, and respond to these actio
ment must also carefully examine what

**Cybersecurit
Practices
for the
Safety of
Modern Vehi**

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

U.S. FOOD & DRUG
ADMINISTRATION

← Home / Medical Devices / Digital Health Center of Excellence / Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)

Cybersecurity in Medical Devices Frequently
Asked Que

Share Tweet in

Digital Health Center of Excellence
Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)
About the Digital Health Center of Excellence
Digital Health Center of Excellence Services
Ask a Que
Health Re
Jobs in th
Center of
Network o
Experts
What is D
Cybersecu
Digital He
Guidance
Health Co
Digital He

This page provides answers to frequently
cybersecurity in medical devices.

On December 29, 2022, the Consolidate
signed into law. Section 3305 of the Om
Devices" -- amended the Federal Food, I
section 524B, Ensuring Cybersecurity of
Omnibus, the requirements of section 5
submission submitted to the Food and I
2023. For devices submitted after March
issue "refuse to accept" (RTA) decisions
that are submitted before October 1, 20

ACQUISITION.GOV

Home > Regulations > DFARS > 252.239-7018

DFARS
Change Number: DFA
Effective Date: 04/27/

Part 252
252.2
252

252.239-7018 Supply

As prescribed in 239.7306 (b), use the following clause:

SUPPLY CHAIN RISK (DEC 2022)

(a) *Definitions*. As used in this clause–

"Information technology" (see 40 U.S.C 11101(6)) means, in lieu of the definition at FAR 2.1, any
equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the autom
acquisition, storage, analysis, evaluation, manipulation, management, movement, control, displa
switching, interchange, transmission, or reception of data or information by the agency.

(1) For purposes of this definition, equipment is used by an agency if the equipment is us
agency directly or is used by a contractor under a contract with the agency that requires—

(i) Its use; or

(ii) To a significant extent, its use in the performance of a service or the furnishing of a

(2) The term "information technology" includes computers, ancillary equipment (includin
peripherals, input, output, and storage devices necessary for security and surveillance), periphe

Office of
POLICY

ABOUT US OUR OFFICES NEWS OPPORTUNITIES

Securing America's Clean Energy Supply Chain

Office of Policy » Securing America's Cl

In February 2022, the U.S. De
"**America's Strategy to Sec
Energy Transition**"—the firs
build an Energy Sector Indu
technologies and crosscutti
Executive Order 14017 on A
whole of government appro
U.S. economy and domestic
most critical supply chains.

The energy sector has under
cost reduction and increase
widespread uptake of efficie
and strain on our electric gr
electric cars, trucks, and bu

In the decades to come, the
pace reflecting continued in
capital markets, and the urg
change. Demand for clean e
dramatically as we work tow
emissions in half by 2030, c
2035, and achieve net zero e
2050.

NIST Special Publ

Secure Software D
Framework (SSDF) V

*Recommendati
the Risk of Softwa*

This publication is availa
https://doi.org/10.

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Administration

MARCH 02, 2023

FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy

BRIEFING ROOM ST

Read the full st

Today, the Biden-Harris Administra
Cybersecurity Strategy to secure th
digital ecosystem for all Americans
United States will reimagine cybers
in a way that reflects our values: ec
respect for human rights and funda
democracy and democratic instituti
society. To realize this vision, we m
how the United States allocates rol
in cyberspace.

1. We must **rebalance the responsi**
   shifting the burden for cybersecu
   businesses, and local government
   are most capable and best-positio

2. We must **realign incentives to fa**
   striking a careful balance betwee
   urgent threats today and simulta
   and investing in a resilient future

The Strategy recognizes that gover
national power in a coordinated ma
security, public safety, and economi

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

June 9, 2023

M-23-16

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young Shalanda D. Young

SUBJECT: Update to Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*

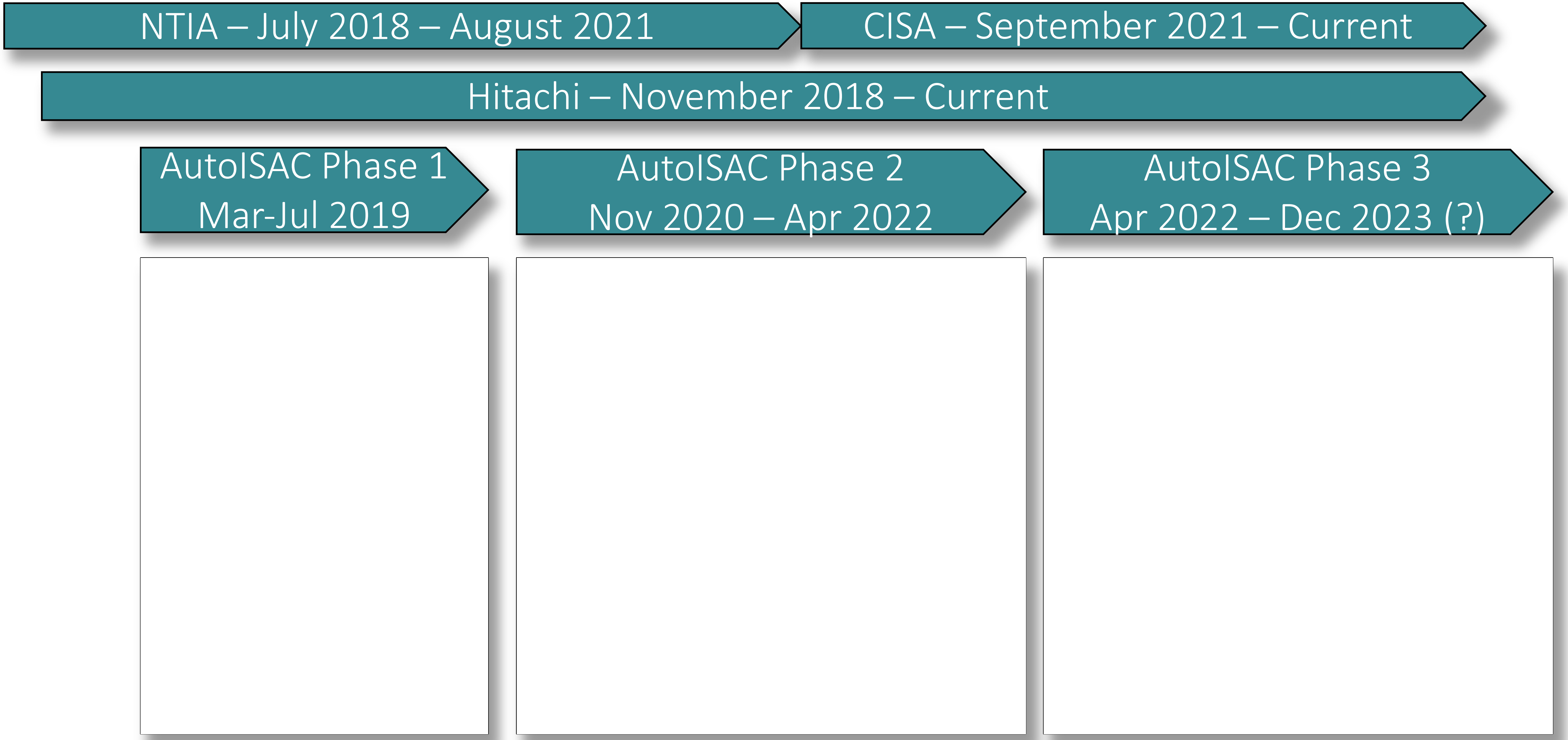
Introduction and Authorities

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021),[1] focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs agencies to take a variety of actions that "enhance the security of the software supply chain." In accordance with the EO, the National Institute of Standards and Technology (NIST) has released the NIST Secure Software Development Framework (SSDF), SP 800-218, and the NIST Software Supply Chain Security Guidance (hereinafter, referred to collectively as "NIST Guidance").[2] OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (M-22-18) (Sept. 14, 2022), requires agencies to comply with that NIST Guidance. Pursuant to M-22-18, agencies must only use software that is provided by software producers who can attest to complying with Government-specified minimum secure software development practices.

This memorandum reinforces the requirements established in M-22-18, reaffirms the importance of secure software development practices, and extends the timelines for agencies to collect attestations from software producers. Additionally, this memorandum provides supplemental guidance on the scope of M-22-18's requirements and on agencies' use of Plan of Actions and Milestones (POA&Ms) when a software producer cannot provide the required attestation, but plans to do so. To the extent any provision of this memorandum may be read to conflict with any provision of M-22-18, this memorandum is controlling.

[1] Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-onimproving-the-nations-cybersecurity/
[2] NIST Secure Software Development Framework (SSDF) SP 800-218; NIST Software Supply Chain Security Guidance under Executive Order (EO) 14028 Section 4e.

Auto-ISAC SBOM Working Group – 3 Phases



NTIA – July 2018 – August 2021

CISA – September 2021 – Current

Hitachi – November 2018 – Current

AutoISAC Phase 1
Mar-Jul 2019

AutoISAC Phase 2
Nov 2020 – Apr 2022

AutoISAC Phase 3
Apr 2022 – Dec 2023 (?)

Phase 1 and 2: NTIA Input / Info. Report

Phase 1: Questions for the NTIA:

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: Information Report For Members:

INCLUDED:

TLP AMBER distribution
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

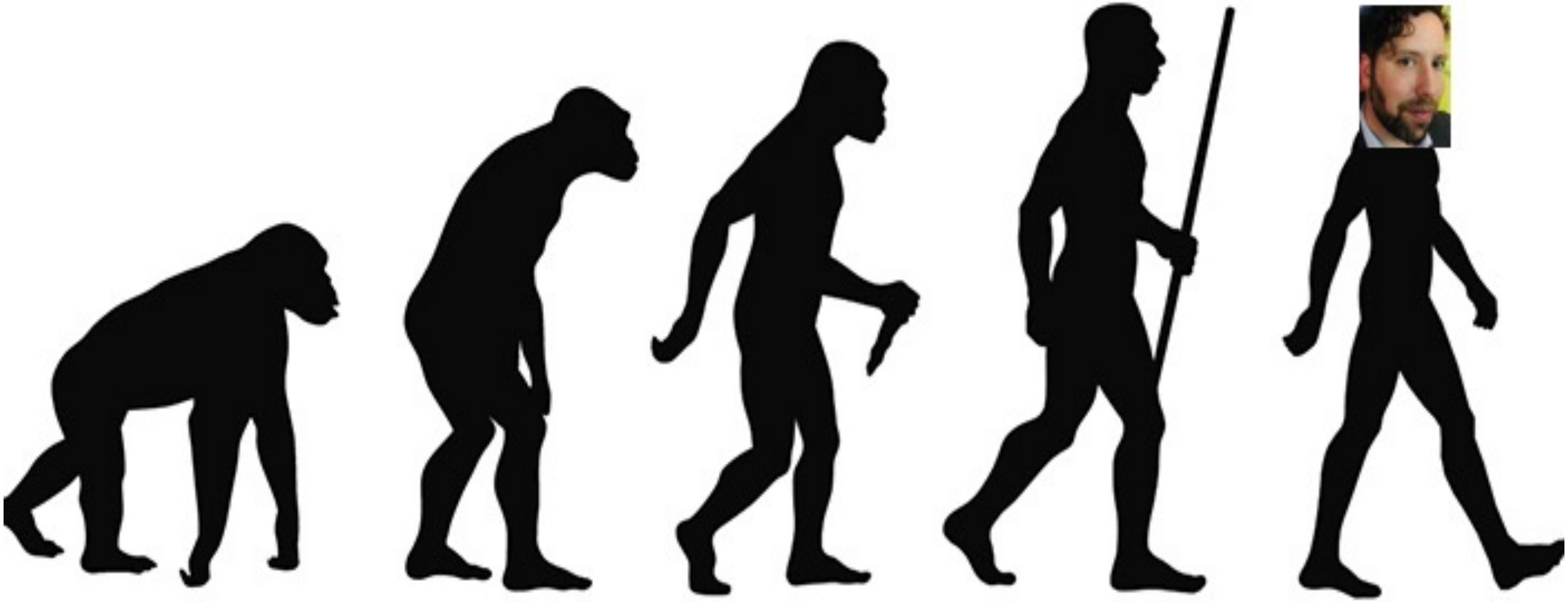
EXCLUDED:

Mandatory rules – all points are recommendations

Usurpation of supplier contracts or requirements

Static guidance – revisions expected during Phase 3 and ongoing

Phase 3: Operations Practice

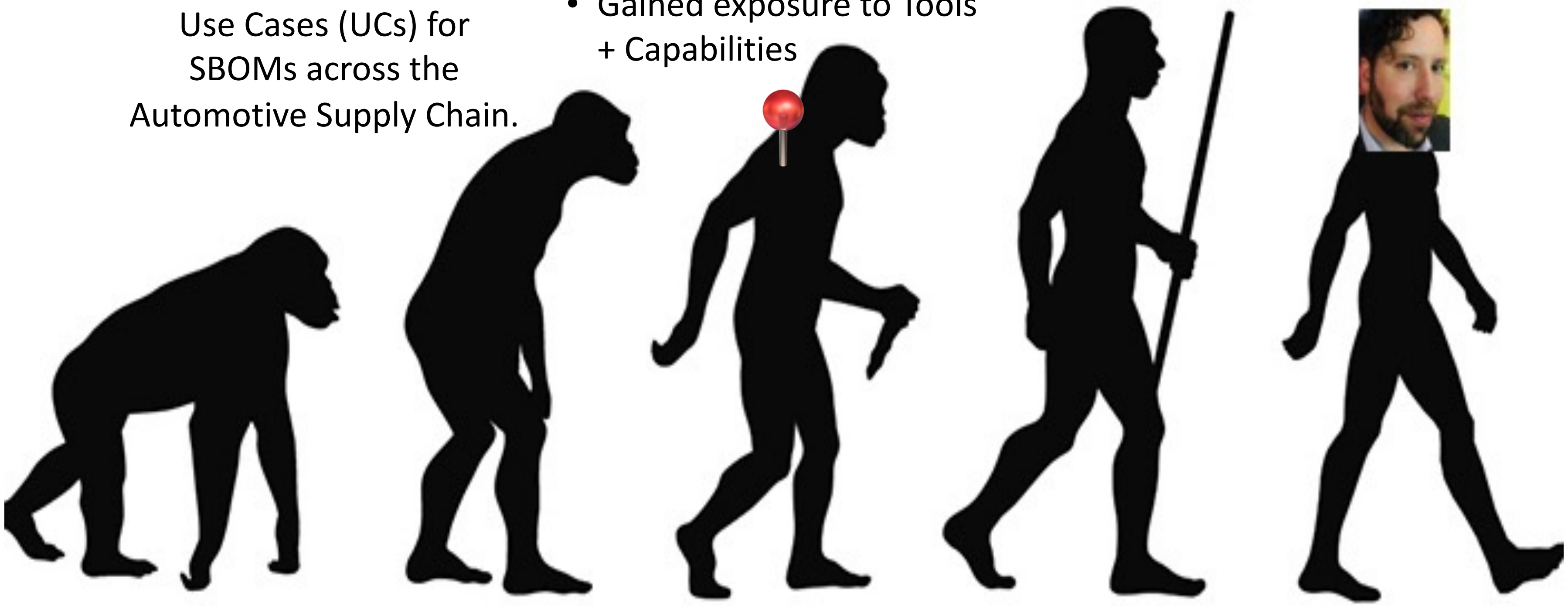


Phase 3: Operations Practice

Developed and Agreed Use Cases (UCs) for SBOMs across the Automotive Supply Chain.

- Conducted exercises on most valuable UCs
- Built understanding
- Identified findings, key issues, challenges
- Gained exposure to Tools + Capabilities

- Conduct 3rd exercise
- Update UCs
- Build consensus
- Identify issues
- Issue a final report



📍 = We are here

Phase 3 – Operations Practice – Discussion and Exercises

- TLP:AMBER Members Only – Confidential
- Agreement: List of use cases and generic "actors" for automotive SBOMs.
- Agreement: Conduct exercises that expose SBOM operations requirements and pitfalls
- Agreement: Write a paper with findings including updates of previous WG documents
- Two exercises were held and another is planned for late 2023

Round 1 – January:

- **Create**
- **Transmit & Receive**
- **Store & Assess Quality**
- **Scan & Review**

Round 2 - May:

- **Create**
- **Name**
- **Transmit (min requirements)**
- **Analyze**

80 member attendees (40 on site, 40 virtual)
10 OEMs, 20 Suppliers

- Sharable Findings:
  - **Tremendous and growing interest from members, ~$1.5 Trillion company revenue represented**
  - **Tools** are more advanced than expected but still have gaps and quirks
  - **Product** (i.e. onboard vehicles) requires different management techniques from IT and OT
  - **Safety** impacts continue to be the top concern both for vulnerabilities and mitigations (Enterprise impact can also be significant)
  - WG members would like to find a consensus across the supply chain for SBOM operations – cannot mandate however

Auto-ISAC SBOM WG Exercise: *New!* Vendor Day

Call for Participation:

- CISA Tooling & Implementation workstream
- Other SBOM tool vendors known to Auto-ISAC SBOM WG members

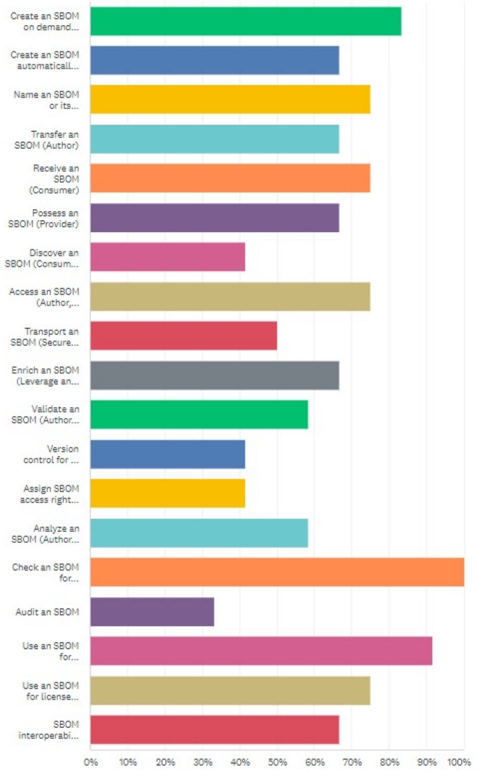
Statistics

- 13 vendors responded | 12 with commercially available tools | 1 with tool currently under development
- First 10 vendors to respond presented
- Survey responses + pre-read materials sent to members in advance
- 50+% of responding vendors have SBOM tools that address potential automotive use cases
- 10 minute overview + live demo
- 90 minutes for in person, virtual or hybrid Q&A with members

26 vendor attendees (7 on site, 19 virtual)
10 vendor companies

Check all potential automotive use cases for your SBOM tool (see CISA + DOE SBOM Sharing Lifecyle Report https://www.cisa.gov/resources-tools/resources/software-bill-materials-sbom-sharing-lifecycle-report)

Answered: 12 Skipped: 1



What Worked

- Structured format + Live tool demonstrations + Well-respected presentation time limits
- Understand the maturity of the SBOM tool industry and see demos of their tools
- Understand vendor capabilities, maturity, interfaces and focus areas
- Understand which vendors are interested in working with Automotive
- Hybrid format

Needs Improvement

- Pre-read was for the “fluff,” live presentation was for show & tell
- 15-30 minutes instead of 10 for more demo
- Some participants did not realize they could request deeper dive/demo during Q&A
- Europe-friendly date + time

Thank you! Questions?