

## SBD Explores: Automotive SBOMs

# Leveraging automotive SBOMs to enhance security and traceability

### 10-minute Insight

Initially, Software Bill of Materials (SBOM) were developed outside of the automotive industry to handle software license compliance. The benefits of SBOM for vulnerability tracking have since been broadly recognized and are now being deployed as part of the effort to secure the Software-Defined Vehicles (SDVs) of the future.

In this edition of SBD Explores, we will dive into the status of SBOMs in the automotive industry, look at their benefits and limitations (both inside the automotive enterprise as well as the broader software ecosystem), and share where they need to go to keep vehicle software safe.

#### Target audience

Cybersecurity Engineering

SDV/Software

#### Focus market(s)

Global



# What is happening?



## What is a SBOM?

- SBOM stands for Software Bill of Materials, like a bill of materials used in manufacturing.
- SBOMs list the detailed collection of components and dependencies that make up a software package.

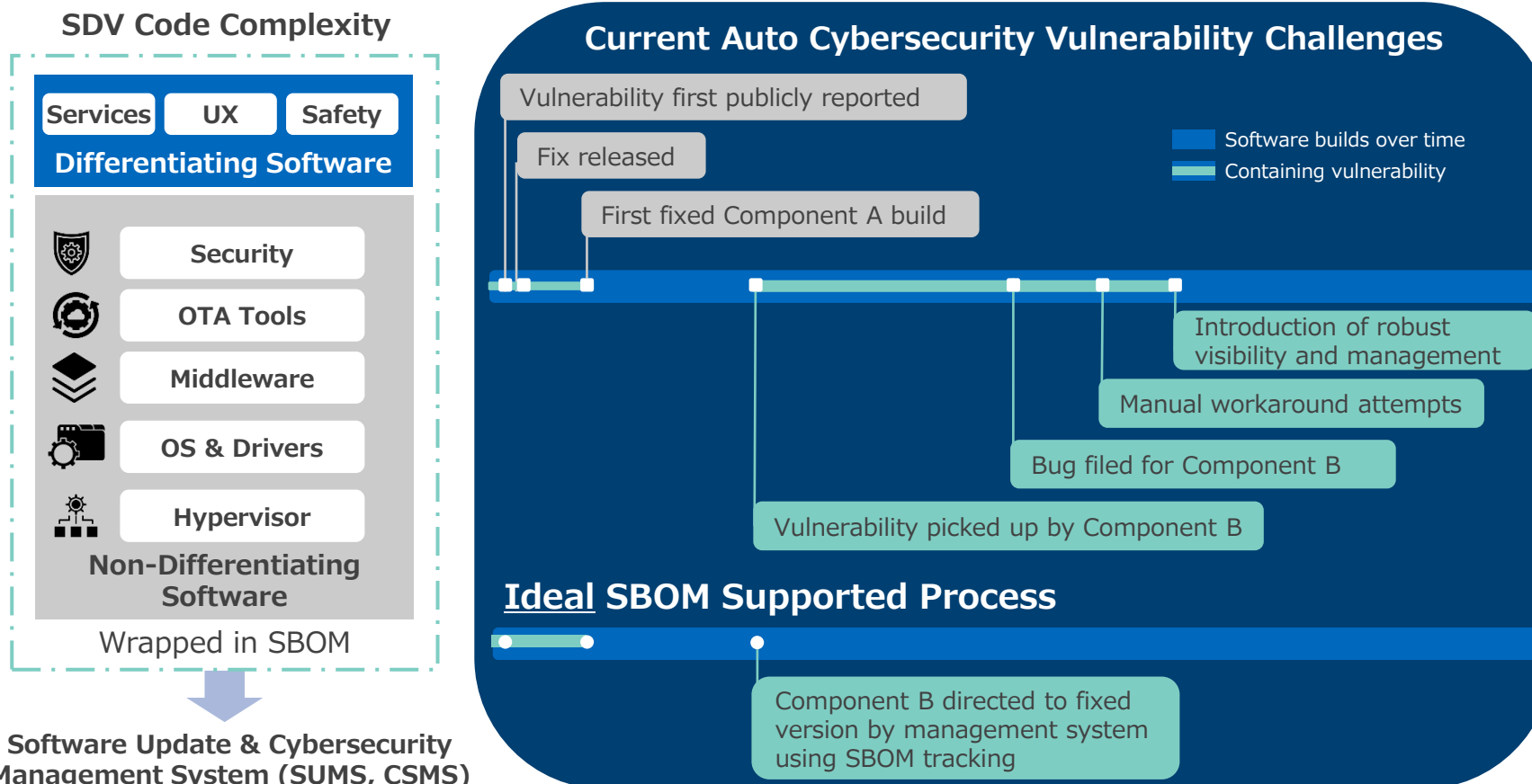
## Role of SBOMs for OEMs

- Automakers and their partners are facing a new value chain with Software-Defined Vehicles (SDVs). SBOMs document that value chain and enable the separation of software, from hardware configuration management. SBOMs can be updated as new features and services are approved and deployed.

## Key takeaway

**SBOMs are a machine-readable format that enable important quality tracking and verification processes.**

- Modern vehicles contain software components from OEMs, suppliers, and third parties. This requires strong documentation to ensure traceability.
- Automakers can compare SBOMs with vulnerabilities. This enable the application of faster fixes or the choosing of appropriate mitigations. Common Vulnerabilities and Exposures (CVEs) can be identified, and affected modules can be blocked from reuse.
- Across ecosystems, SBOMs can help verify the software libraries used. Partners have had challenges ensuring that only fixed versions are used by future components.
- Though not automotive, the Log4j/Log4Shell software flaw in 2021-2022 was discovered in a widely-used, open-source Java development library. Remediation challenges taught all cyber departments the importance of tracking and controlling versions of libraries used in released products.
- SBOM has seen significant interest and implementation from automotive OEMs to address supply chain security issues.



# Why does it matter?



## Why is change needed?



**Complexity:** With the growing number of vehicle platforms embracing the Software-Defined Vehicle (SDV), not only is a larger amount of software needed to run the vehicle, but system and code interactions are more complex and interdependent.






**Expectations:** Increasingly, general purpose software and automotive-specific regulations look to Software Bill of Material (SBOM) documentation to ensure included software is identified and able to be tracked against vulnerability disclosure databases.



**Risk management:** Over-the-air (OTA) updates can increase the chance of a cybersecurity attack due to the vehicles being connected to the cloud. Adhering to SBOM best practices will help document that OEMs are following their duty of care.

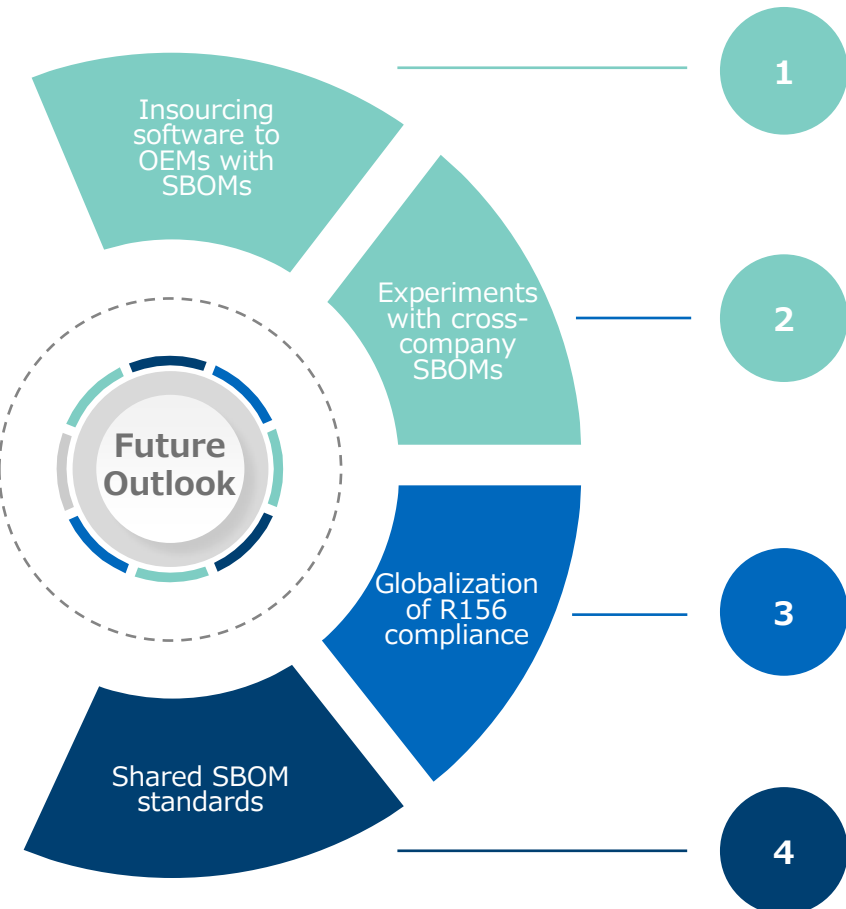
## What are the key regulatory impacts to consider?

Region	Regulator	General	Automotive	Best Practices
<b>USA</b> 	The White House	✓		Executive Order 14028 has required all software vendors to the federal government to provide SBOMs since May 2021
	National Highway Traffic Safety Administration		✓	SBOMs are included in NHTSA's 2022 "Cybersecurity Best Practices for the Safety of Modern Vehicles"
<b>Europe</b> 	United Nations Economic Commission for Europe		✓	UNECE Regulation 156 requires manufacturers to implement a software update management system to document safety of the vehicle and its occupants, including version tracking
	European Commission	✓		The "Cyber Resilience Act" requires the use of SBOM by vendors and producers of software
<b>China</b> 	MIIT (中国工业和信息化部)	✓	✓	The Ministry of Industry and Information Technology of China published a guide for security risk management in the connected car supply chain - other activity is ongoing

## Key takeaway

**While regulators currently use SBOM as a 'check item', security goals will be gained by thoughtful integration.**

- OEM software management must fit complex regulatory frameworks. Managing the growing software source code and binaries from suppliers, consortia and in-house needs standard formats and tools.
- Supply chain attacks show the need to verify the authenticity of software sources. SBOM provides efficient methods across projects and across industries.
- Regulations and best practice guidance push manufacturers toward good cybersecurity practices. OEMs need to implement the processes to maximize the benefits, while minimizing the cost.
- SBOMs help quickly propagate implemented fixes, if the SBOM system is embedded in development and update processes.
- Rather than a tool to assign blame between OEMs and suppliers, SBOMs should speed up fixes, and prevent known vulnerabilities from being distributed.



1 As OEMs build more software in-house for next generation Software-Defined Vehicles, internal SBOMs can be better tracked to ensure known vulnerabilities are fixed before release.

2 OEMs are experimenting with the use of SBOMs with trusted partners. This is to provide increased traceability from first vulnerability news to accelerated repair of affected systems, and services, across their supply chain.

3 SBOMs meet the requirements of R156 and improve robustness of over-the-air updates.

4 In the long term, consumers will benefit from quicker updates and less recalls via OEM SBOM standardization for common middleware to better secure the vehicle ecosystem.

## Key takeaway

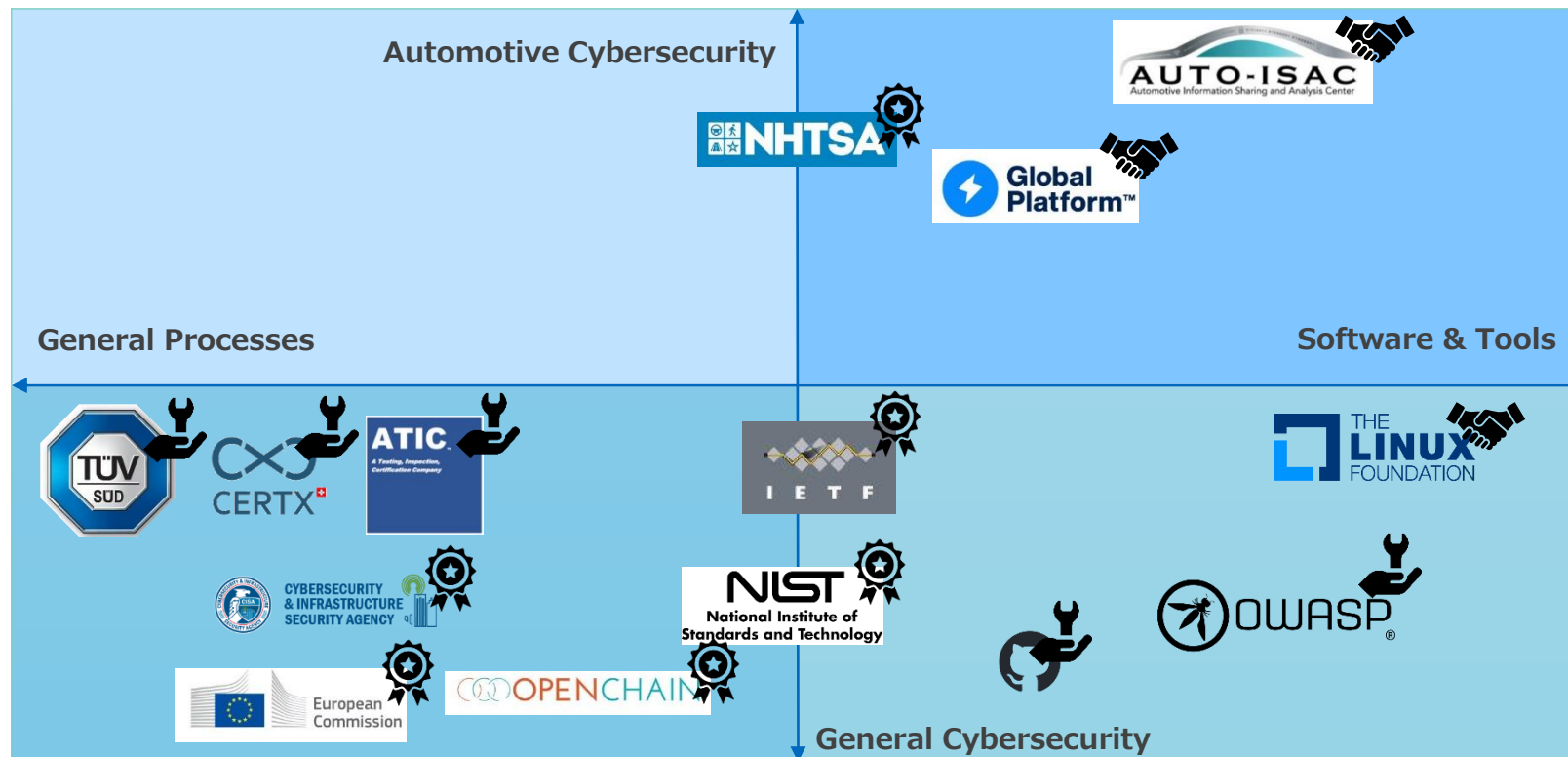
**OEMs can use the Software-Defined Vehicle transformation to more clearly identify and efficiently protect the value creation of automotive software.**

- As OEMs increase their participation in the software value of automobiles, they are gaining deeper understanding of software system dependencies within and outside the organization. This understanding includes tracking licenses, original authors, and current maintainers of software packages.
- In the near term, SBOM generation by scanning existing code will highlight areas of concern to system module integrators. As software authors add SBOM to their development flows, increased visibility to the relative risks of dependency options will improve system robustness.
- Automotive processes are increasingly reliant on SBOMs as documentation that cybersecurity verifications were completed. As R156 expands to more models and regions, simplifying reuse within a company will gain in importance.
- Suppliers will gain efficiencies if SBOM documentation can scale across multiple systems and OEMs.

# Who to watch out for?

## Standards bodies, industry consortiums and commercial test houses & tool providers are laying the groundwork for SBOM adoption

- Standards Bodies & Regulators: SBOM benefits from greater standardization specifying SBOM formats (ISO/IEC 5926) and in SBOMs being accepted by certification bodies to meet other standards and regulations (SAE/ISO 21434, UNECE 156).
- Industry Consortiums: How SBOMs can be best applied to specific automotive environments is being deliberated and tested as OEMs implement them into larger processes and frameworks.
- Test Houses & Tool Providers: SBOMs allow a common language for communication of software contents, enabling new tool integrations, verification processes and source monitoring.



## Key takeaway

**Certification bodies and standards organizations are partnering with the automotive industry to achieve increasing levels of cybersecurity via collaboration.**

- OEMs need to improve SBOM processes to meet the requirements of future type approval regulations.
- Certification bodies expect the continuous improvements needed to meet ever increasing cybersecurity challenges. It is a mistake to think that the same methods used for approvals today will be enough for the future.
- Auto-ISAC and GlobalPlatform are two examples of organizations with automotive SBOM working groups.
- Generic SBOM formats, protocols, and standards continue to be refined based on industry feedback and changing technologies.
- Further requirements and recommendations, depending on robust SBOM implementations, are expected.

# How should you react?



# 1

## Embrace

Embrace SBOM deployment and development by enabling company-wide and ecosystem software module version and control.

# 2

## Implement

Leverage SBOMs to 'shift left' to take advantage of improved traceability resulting in fewer vulnerabilities and faster patching.

# 3

## Collaborate

Identify industry consortiums and tool supplier partners to optimize deployment of existing SBOM solutions and processes for automotive applications.

## Authors



**Jeffery Hannah**  
Chief Commercial Officer



**Andrew Wilczynski**  
Research Analyst

## Related SBD Reports



**Ref: 404**  
Securing The  
Software-  
Defined  
Vehicle



**Ref: 905**  
Cyber  
Intelligence  
Guide

## Related SBD Consultancy

- Automotive Cybersecurity Advisory
- Penetration Testing
- UNECE R155/R156 Compliance
- Threat Assessment and Remediation Analysis (TARA)

## Interested in finding out more?

If you would like to discuss recent cybersecurity projects that we have completed, and how to secure the Software Defined Vehicle, please [contact us](#).