# Automotive Software Supply Chain Security

## Traceability, Country of Origin & Industry Alignment

Amadou Kane

xBOM

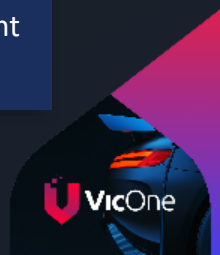
COO

**97%**

of vehicles: software from 3+ countries

**2026**

U.S. COO rule enforcement deadline



# Supply Chain Security Is Now a National & Industrial Risk

STRATEGIC CONTEXT

### Deeply Nested, Global Sourcing

Modern vehicles now embed over 100 million lines of code sourced globally, making the origins of their software, firmware, and silicon increasingly difficult to trace. No single entity has full visibility.

### Trust Assumptions Are Exploited

Attackers leverage weak traceability, jurisdictional blind spots, and inherited trust in supplier attestations. 'Unknown origin' does not mean safe.

### Scale & Speed of Systemic Failure

Supply chain compromises propagate across every system that consumed the affected component.

### Traceability Answers Four Critical Questions

**WHAT** components are in the system?

**WHERE** did they come from — origin, jurisdiction, ecosystem?

**WHO** influenced or maintained them?

**HOW** were they built, delivered, and modified?

***Traceability is the foundation of trust.***

# How Supply Chains Are Being Exploited

THREAT LANDSCAPE

## Observed Attack Patterns

**01 Compromised OSS Dependencies**

Malicious packages injected into widely used open-source repos — exploiting transitive trust in library ecosystems.

**02 Build-Time Injection**

Toolchain compromise inserts backdoors during compilation. The artifact is clean in source; malicious at execution.

**03 3rd Party Integration**

Integrating third-party technologies has expanded the attack surface, introducing unforeseen risks.

## Emerging Reality

**"Unknown origin" ≠ Safe**

Absence of provenance data is itself a risk signal. Attackers deliberately obscure origin.

**Provenance = Vulnerability Severity**

Software origin is now as critical a risk factor as CVE score.

**Compliance & Security Gaps = Attack Surface**

Organizations with incomplete SBOMs cannot verify what they're running.

**COO Determination Requires Technical Validation**

Repackaging, and embedding all obscure true origin.

# Supply Chain Risks Across the Development Lifecycle

LIFECYCLE RISK

| DESIGN | BUILD | INTEGRATION | DEPLOYMENT | MAINTENANCE |
| --- | --- | --- | --- | --- |
| **Unvetted Dependencies** | **Compromised Toolchains** | **Transitive Blind Spots** | **Non-Compliant Components** | **Silent Replacement or Drift** |
| Third-party libraries selected without origin review. Dependency trees inherited without analysis. | Compiler, linker, or CI environment tampered. Malicious code inserted post-review, pre-artifact. | Dependencies of dependencies are never inventoried. | Undetected prohibited-origin software ships in production. Firmware images contain unverified binaries. | OTA updates alter software composition post-certification. Component origin can change without alerting. |

# COO Compliance Is No Longer Optional

## THE REGULATORY LANDSCAPE

**2021**

**EO 14017**

Executive Order on America's Supply Chains mandates software transparency across critical sectors.

**2022**

**CHIPS & Science Act**

Restricts semiconductor procurement from entities linked to China and Russia.

**2023**

**NDAA §5949**

Prohibits connected vehicle software from ICTS supply chains with ties to adversarial nations.

**2024**

**BIS Rules (ICTS)**

Commerce Dept finalizes rules restricting Chinese/Russian/Iranian/North Korean/Cuban software in connected vehicles.

**2026**

**Enforcement Active**

Full COO disclosure requirements take effect. Non-compliance risks fines, market exclusion.

# Visibility Breakdown

SOFTWARE TRACEABILITY

## What Full Traceability Requires

01 Component-level SBOM in standardized format (SPDX 2.3 / CycloneDX 1.5)

02 Origin metadata: source repo, maintainer entity, signature, country registration, ownership

03 Binary-to-source linkage across compiled firmware and libraries

04 Continuous monitoring: components change post-build via OTA updates, and landscape is dynamic

05 Cross-reference against OFAC, EAR Entity List, and ITAR control lists

06 Audit-ready reporting aligned to BIS and ISO/SAE 21434

# Standards, Frameworks & Regulations

INDUSTRY ALIGNMENT FRAMEWORK

| NIST Frameworks | Automotive Standards | U.S. Regulatory Requirements |
| --- | --- | --- |
| **NIST SP 800-161r1**<br>C-SCRM practices: defines tiered supplier obligations, assessment criteria, and risk categorization for software components | **ISO/SAE 21434**<br>Cybersecurity engineering for road vehicles: mandates TARA covering third-party components | **ICTS Final Rule (BIS)**<br>Bureau of Industry & Security prohibits connected vehicle software and hardware with Chinese, Russian, Cuban, North Korean, or Iranian components |
| **NIST SSDF (SP 800-218)**<br>Secure Software Development Framework: requires source/origin documentation from all third-party library suppliers | **UNECE WP.29 / R155**<br>Global market entry requirement (EU, Japan, Korea). CSMS certification requires documented supply chain controls | **NDAA §5949**<br>Defense authorization language bans covered software in federal vehicle fleets |
| **NIST CSF 2.0 — GV.SC**<br>New Govern function explicitly addresses supply chain risk governance as a board-level accountability | **SAE J3061**<br>Best practice guidelines for automotive cybersecurity; superseded by ISO/SAE 21434 update | **EO 14028 (Cyber EO)**<br>Requires software bill of materials and source for all software used by federal agencies and their supply chains. |

# From Trust Assumptions to Trust Evidence

SECURE COMPONENTS

## Secure Component Characteristics

**Verifiable Origin**

Country, legal entity, and ecosystem of development confirmed through technical analysis, not supplier declaration alone.

**Transparent Dependency Structure**

Full SBOM with transitive dependencies declared and verifiable — not just top-level packages.

**Traceable Build & Update Lineage**

Binary artifacts linked to source, compiler, toolchain, and signing entity.

**Regulatory Framework Alignment**

Component cleared against OFAC, EAR Entity List, ITAR, and sector-specific controls at integration time.

## The Required Shift

*From: Supplier attestation — 'We certify our software is compliant'*

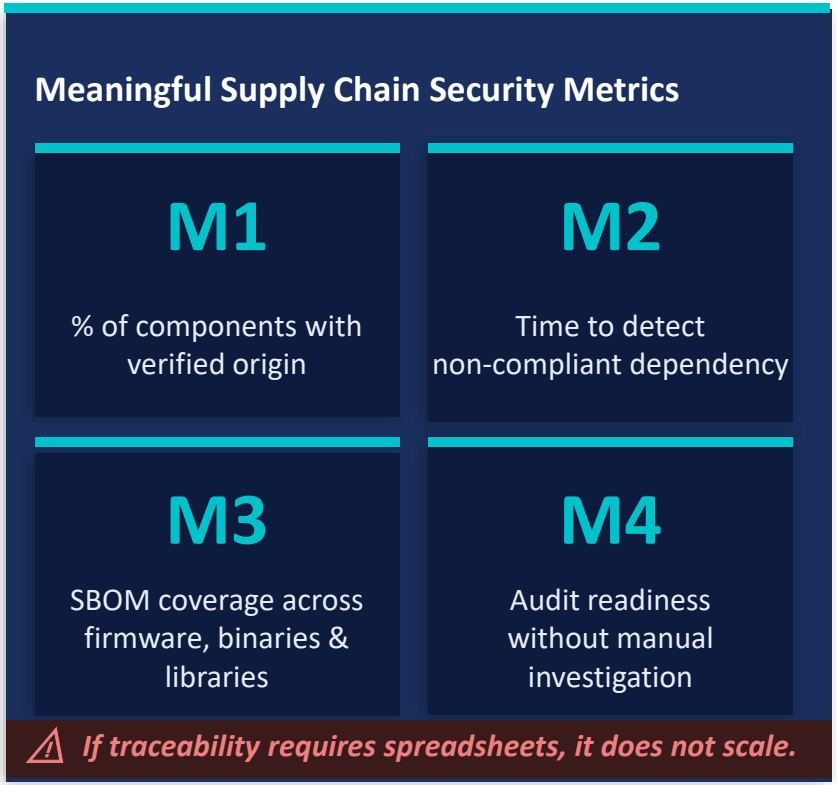
**To: Independent, repeatable technical verification of every component**

## Four Industrial Alignment Areas

| | |
|---|---|
| I | **Traceability-First Architecture**<br>Binary/firmware analysis + dependency mapping |
| II | **Jurisdiction & Compliance Intelligence**<br>Sanctions controls, geographic & ecosystem risk tracking |
| III | **Multi-Layer Verification**<br>Metadata, structure, encoding, Signature, Certs, Network |
| IV | **Workflow Integration**<br>Embed decisions into procurement and CI/CD pipelines |

# Metrics

MEASUREMENT



# The Road Ahead

Securing the automotive software supply chain requires a whole-of-industry approach.

*Organizations that invest early in traceability gain strategic resilience and the ability to respond rapidly to geopolitical shifts.*

## Takeaways

1. **Visibility is the prerequisite**

   You cannot secure what you cannot trace. SBOM traceability to Tier-N is non-negotiable.

2. **Standards fragmentation is the threat**

   Without harmonized COO attestation standards, compliance will be uneven and enforcement inconsistent.

3. **Trust must be earned technically**

   Supply chain trust cannot be assumed contractually. Independent, repeatable verification is the only defensible standard.

VicOne

***You cannot secure what you cannot trace. You cannot trace what you cannot see. Supply chain trust must be earned technically.***