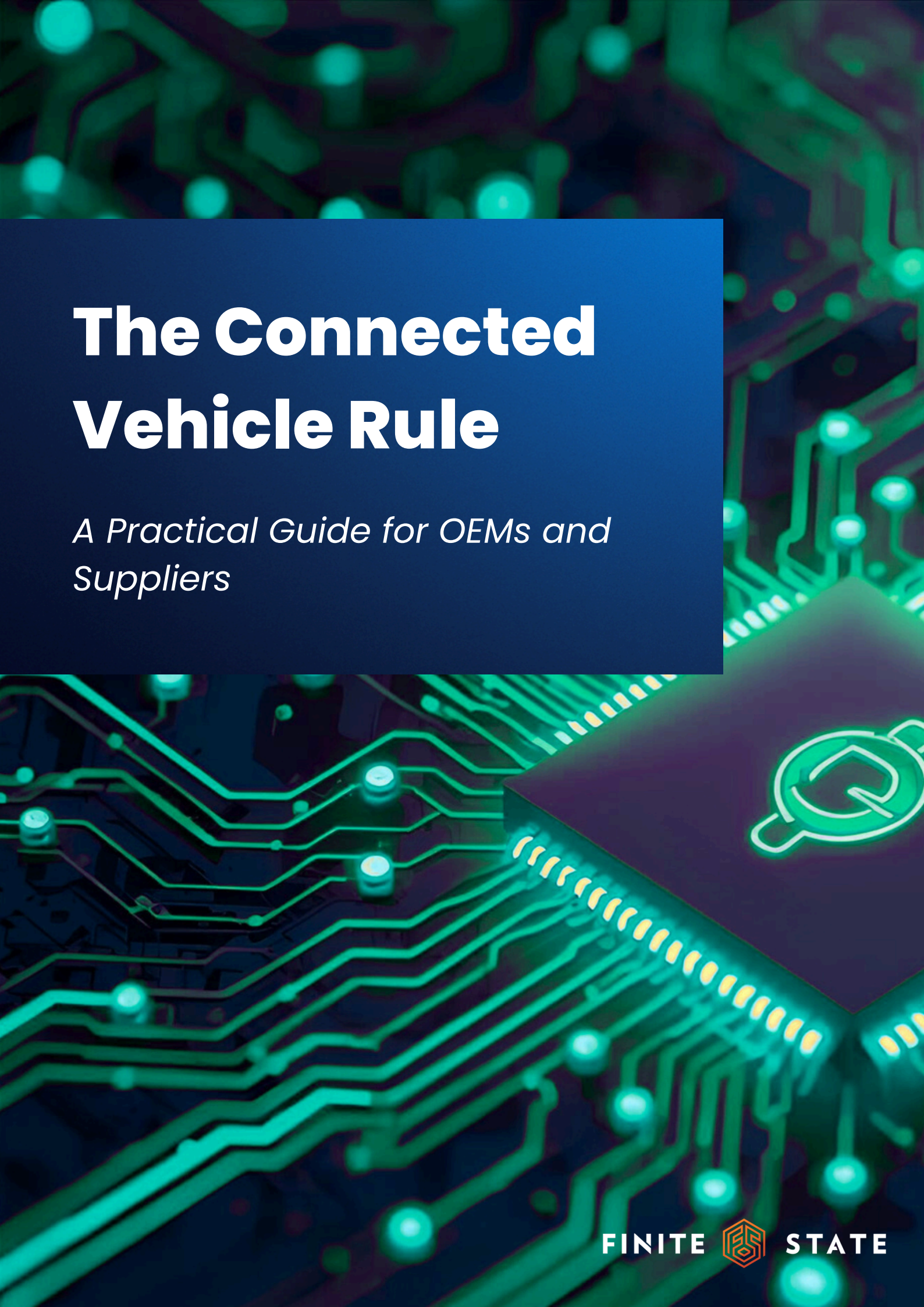


The Connected Vehicle Rule

A Practical Guide for OEMs and Suppliers

FINITE STATE

Contents

CVR 101: What It Is & Why It Matters

The Connected Vehicle Rule (CVR), published by the U.S. Department of Commerce in January 2025, represents one of the most consequential regulatory changes the automotive industry has faced in decades. It is the first regulation to explicitly restrict the use of certain vehicle software and hardware based on the origin of the technology, targeting components tied to foreign adversaries — specifically China and Russia.

The CVR falls under the Department's authority over Information and Communications Technology and Services (ICTS), derived from the International Emergency Economic Powers Act (IEEPA). This is the same legal foundation that supports U.S. sanctions programs. The automotive sector now finds itself subject to a regulatory framework originally designed for telecommunications and national security, demonstrating an expansive approach to implementing this authority.

The rule applies not just to electric vehicles or cutting-edge autonomous platforms but to equipment that is present in virtually every vehicle produced in the last ten years. This includes modern telematics, infotainment systems, over-the-air (OTA) updates, and vehicle-to-infrastructure (V2X) functions all qualify as connectivity features. As a result, OEMs, their suppliers, and aftermarket telematics vendors are all implicated.

> This rule is one of the most consequential auto regulations in decades. It's requiring folks to exercise muscles they've never had to exercise before.
>
> Hillary Kane, Alliance for Automotive Innovation

The CVR Prohibits:

- Importing vehicle connectivity system (VCS) hardware designed, developed, manufactured, or supplied by entities under the jurisdiction or direction of China or Russia.
- Importing completed vehicles that incorporate "covered software" linked to those same entities.
- Knowingly selling vehicles that include such covered software.
- Selling vehicles in the U.S. if the manufacturer itself is subject to Chinese or Russian jurisdiction.

These prohibitions are enforced through an annual Declaration of Conformity. Each importer or manufacturer must certify they have conducted the necessary due diligence to ensure compliance

For industry leaders, the CVR is not just another compliance box to check. It demands a fundamental rethinking of supply chain visibility and risk management.

In short: the Connected Vehicle Rule is not only about regulatory enforcement. It is a strategic turning point that requires immediate action to assess supply chains and document security in order to maintain market access.

Key Definitions & Ambiguities

While the CVR is sweeping, its language introduces significant ambiguity. This is by design: the Department of Commerce aimed to cast a wide net to capture emerging risks. But for OEMs and suppliers, the lack of precise definitions creates practical challenges. Below, we break down the most important concepts and highlight areas of uncertainty.

Owned or Controlled By

The rule prohibits hardware and software "owned or controlled by" entities in China or Russia. This goes far beyond majority ownership. It can include:

- Minority investments or board representation.
- Licensing arrangements.
- Jurisdictional control, where an entity is legally subject to adversary government direction.

Covered Software

Software associated with VCS or ADS functionality. This includes:

- Telematics control firmware.
- OTA (over-the-air) update systems.
- Autonomous driving algorithms at Level 3 or above.

It does not include peripheral or support functions unrelated to connectivity or autonomy (e.g., wipers, brakes).

Declaration of Conformity

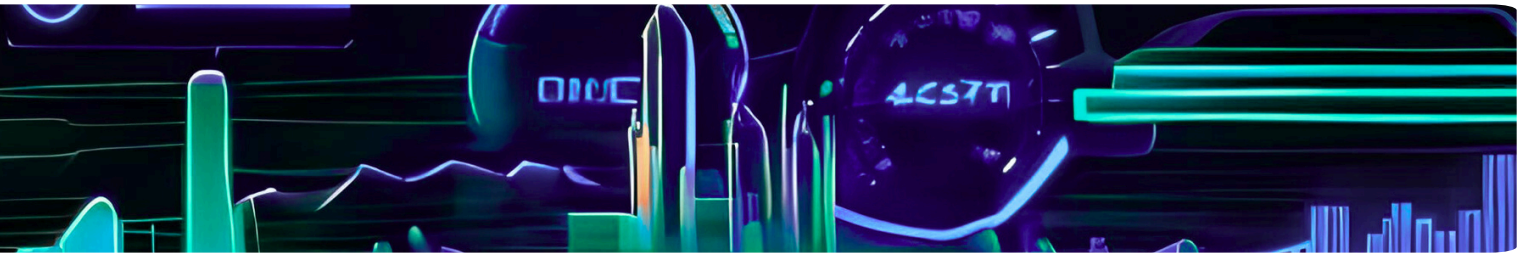
Each year, importers and manufacturers must either file a Declaration affirming they have conducted due diligence to ensure compliance or submit a request for Specific Authorization (to engage in an otherwise prohibited transaction). Either filing must be backed by documentation — SBOMs, HBOMs, ownership analyses, and vulnerability assessments. These documents must be retained for ten years.

Directly Enable

The CVR applies to components that "directly enable" VCS or ADS functions. But where is the line drawn?

- Clearly in scope for VCS: Components that are software-enabled or programmable AND directly enable the function of VCS, including telematics units, cellular/Wi-Fi/Bluetooth modules, and other wireless communication systems.
- Clearly in scope for ADS: Software-based components that directly enable autonomous driving functions at Level 3 or above, including the application, middleware, and system software executed by the primary processing unit(s).
- Explicitly out of scope: Non-communication hardware (brackets, fasteners), firmware, sensing-only systems (LiDAR, radar for sensing), unidirectional receivers (GPS, AM/FM radio), and power management components.
- Gray areas requiring case-by-case analysis: Middleware with mixed functions, ECUs with both connectivity & non-connectivity features, and software where primary processor execution is unclear.

Compliance in Practice



The CVR requires more than awareness; it requires actionable due diligence.

First, companies must assess the ownership, control, and jurisdiction of each supplier in the chain. This often means tracing relationships several tiers deep, into suppliers with whom OEMs have never directly interacted.

Second, diligence must be technical as well as contractual. Supplier attestations alone are insufficient. Binary and source code analysis are essential to verify the accuracy of SBOMs, uncover hidden dependencies, and identify risks not disclosed by vendors.

Third, companies must generate and maintain Software Bills of Materials (SBOMs). The rule incorporates the NTIA's SBOM standard fields: author, timestamp, component name, supplier name, and supply chain relationships. Equally important are Hardware Bills of Materials (HBOMs), which must list assemblies, parts, and supplier identifiers.

March 17, 2025:
The CVR takes effect. Companies must begin due diligence

March 2026:
Deadline for legacy software carveout eligibility.

Model Year 2027:
Ban on covered VCS or ADS software.

2029/2030:
Ban on covered VCS hardware.

For OEMs operating on multi-year cycles, these dates require action now.

> You are not just responsible for your direct relationship with suppliers. You are responsible for the entirety of that supply chain leading up to you.
>
> Matt Wyckhouse, Finite State

Finally, compliance is long-term. Records must be maintained for ten years, ready to be produced upon request. This requirement ensures that due diligence is continuous, not episodic.

For OEMs, this means building new organizational capacity. Compliance teams must collaborate with engineering, procurement, and legal to design processes that align with both the letter and the spirit of the rule.

The Compliance Roadmap

Compliance with the CVR is a journey requiring deliberate planning. A practical roadmap includes

1. Scoping – Identify all products and platforms with VCS or ADS functions, including aftermarket devices.

2. Visibility – Generate SBOMs and HBOMs. Validate supplier-provided data through independent analysis.

3. Evaluation – Assess ownership, control, and jurisdiction risks. Document findings in audit-ready form.

4. Remediation – Replace or restructure risky components. Pursue specific authorizations where compliance is not an available option.

5. Monitoring – Implement continuous monitoring for vulnerabilities, supplier changes, and compliance status.

This roadmap demands cross-functional effort. Engineering teams must provide technical data, procurement must engage suppliers, compliance must design processes, and leadership must allocate resources.

Exceptions & Transitional Paths

The CVR allows limited exceptions to ease the transition.

The most significant is the Legacy Software Carveout. Software developed prior to March 17, 2026, is excluded from the scope of covered software, provided it is no longer maintained by a Chinese or Russian entity after that date. This carveout creates a narrow window for companies to transfer code maintenance to non-covered entities.

In addition, Specific Authorizations allow companies to petition BIS for case-by-case relief. The bar for approval is high: companies must clearly document rigorous risk assessment and mitigation, often through technical security measures such as robust vulnerability management and penetration testing.

In very limited circumstances (e.g., testing, research), BIS may grant General Authorizations that allow otherwise prohibited transactions to proceed.

These mechanisms provide temporary relief but cannot be relied on long-term. Companies should treat them as stopgaps while moving decisively toward compliance.

Business & Strategic Implications

While the CVR is rooted in cybersecurity, its impact extends across strategy, operations, and market positioning. For many companies, compliance will require supply chain redesigns, renegotiation of contracts, and even restructuring of development programs. These are not short-term adjustments but long-term strategic shifts.

Supply Chain Disruption and Redesign

The automotive supply chain is vast, global, and deeply interdependent. The CVR's lack of a de minimis threshold means that even minimal covered content (i.e., a single line of code) could trigger violations. OEMs will need to evaluate and in some cases replace long-standing suppliers. Tier 1s will face pressure to validate the practices of their Tier 2s and Tier 3s. Procurement functions will need to evolve from price-driven negotiations to risk-informed sourcing strategies.

Aftermarket and Ecosystem Responsibility

Unlike safety recalls, where OEMs typically shoulder the regulatory burden, the CVR places accountability on whoever introduces the component or system into the market. That means aftermarket telematics providers and other ecosystem players must file their own declarations and/or applications. Compliance cannot be outsourced — it is a shared but direct responsibility across the value chain.

Compliance as a Differentiator

While some companies will view the CVR purely as a burden, others will recognize its potential as a market differentiator. By developing a clear compliance strategy, suppliers can provide critical confidence to customers that their procurement decisions will not result in sanctions or denial of access to the U.S. market. Compliance can become a competitive advantage — proof that a manufacturer not only meets the bare minimum but also leads in secure-by-design principles.

In short, the CVR reshapes more than supply chains. It reshapes strategy. The companies that adapt fastest — treating compliance not as a burden but as a foundation for secure innovation — will define the next era of automotive leadership.

FAQs

The Connected Vehicle Rule raises complex, often technical questions for OEMs and suppliers. BIS deliberately drafted the regulation with broad definitions, which means many scenarios fall into gray areas. Below are answers to some of the most common questions we've heard from manufacturers, suppliers, and aftermarket providers with practical guidance on how to approach compliance.

Does the CVR apply only to EVs?

No. The CVR applies to all connected vehicles, regardless of propulsion system. Whether powered by gasoline, hybrid systems, or batteries, if the vehicle includes connectivity features — such as telematics, infotainment, or OTA updates — it is in scope.

What qualifies as "covered software"?

Covered software is any code that directly enables vehicle connectivity or autonomous driving functions at Level 3 or higher. This includes telematics control unit firmware, OTA update platforms, and ADS algorithms. It does not typically include peripheral systems (e.g., wipers, brakes) unless they directly control connectivity or autonomy.

If my supplier is headquartered in Europe but uses developers in China, am I at risk?

Yes. The rule covers not only corporate headquarters but also jurisdictional reach. If software development or maintenance occurs in China or Russia, the component may be considered prohibited. This is why due diligence must go beyond supplier self-attestations to document where code is developed, who maintains it, and under what legal jurisdiction.

Can I rely on the accuracy of supplier-provided SBOMs?

No. Supplier SBOMs are a starting point, but they are often incomplete. Independent verification through binary and source code analysis is essential to uncover hidden dependencies and ensure the SBOM accurately reflects what's in the firmware or software.

What are the penalties for violations?

Companies that fail to comply may face civil and criminal penalties under IEEPA, including fines, loss of U.S. market access, and reputational harm. Because Declarations of Conformity are legal attestations, knowingly or negligently filing inaccurate information could also expose companies to other enforcement actions.

How Finite State Helps You Comply with the CVR

SBOM Management

Automate the generation, ingestion, and management of SBOMs across the entire product lifecycle. Our platform ingests supplier SBOMs, unifies them into a single view, and validates accuracy against binary analysis results, so you can demonstrate possession of SBOMs *and* confidence in their completeness.

Security Scanning & Analysis

Our platform supports both source code and binary analysis, giving OEMs visibility into proprietary, third-party, and open-source components. This dual approach uncovers hidden dependencies that supplier SBOMs often miss, enabling compliance teams to identify and mitigate risks before they become violations.

Reachability Analysis

Filter CVE noise by pinpointing which vulnerabilities are actually exploitable for precision triage that helps teams prioritize remediation efforts — a critical advantage when you must demonstrate not just awareness of vulnerabilities, but active mitigation.

Penetration Testing

Finite State provides regulatory-grade penetration testing of telematics units, head units, and OTA systems. These tests validate resilience against real-world attack vectors, and the results can be used as evidence in BIS-specific authorization requests.

Advisory Services

Our experts — including former U.S. government, legal, and industry leaders — guide clients through the regulatory landscape. From interpreting ambiguous definitions to preparing documentation for Declarations of Conformity, Finite State helps you design a compliance strategy that is both defensible and practical.

Centralized Platform for Evidence

Finite State is your single source of truth for compliance, consolidating SBOMs, HBOMs, vulnerability assessments, pen- testing reports, and supplier attestations into an audit-ready repository. With built-in reporting, you can respond quickly to regulator inquiries and maintain the required 10-year archive.

From Compliance to Leadership

The Connected Vehicle Rule is a signal from the U.S. government that national security and software supply chain integrity are now central to the automotive industry. The deadlines are fast approaching: March 2026 for legacy software carveouts, Model Year 2027 for software prohibitions, and Model Year 2029/2030 for hardware restrictions. For an industry with long development cycles, that leaves little time to act.

Companies that fail to act immediately will face rushed redesigns, supplier disruptions, and regulatory uncertainty. Companies that act now can define defensible processes, build secure supply chains, and differentiate themselves as trusted manufacturers.

Finite State is here to help. We can help guide you through technical, business, and regulatory questions that will enable you to formulate an effective strategy for approaching compliance with the Connected Vehicle Rule. On a tactical level, we are able to support both the collection and assessment of information and documentation required under the Rule. From assessment of individual components to due diligence on suppliers, from SBOM management to binary analysis, from penetration testing to long-term evidence archiving, we provide the tools and expertise to make CVR compliance achievable — and to transform it into a competitive strength.

Next Steps

Don't wait until regulators come calling. **Connect with our team today to begin your CVR compliance journey.**

Learn More

Want to hear directly from industry experts?

Watch our webinar "*From Policy to Action: Expert Advice for OEMs and Suppliers Facing the Connected Vehicle Rule*" for deeper insights into how the rule is reshaping the automotive supply chain.

Watch Now