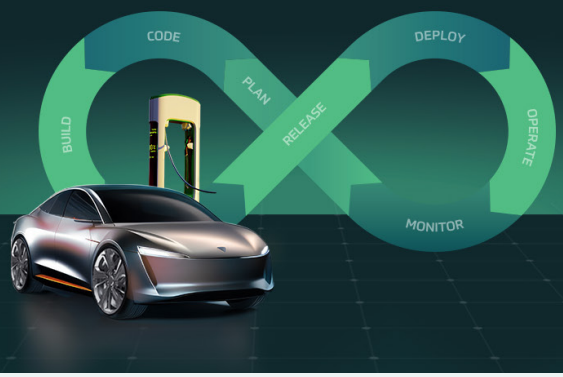
Product Security Regulation Spotlight

C2A security

Department of Commerce Rule

Securing the Information, Communications Technology and Services Supply Chain: **Connected Vehicles**



Rule Snapshot

The Department of Commerce (DoC) rule prohibits transactions involving Vehicle Connectivity System (VCS) hardware and covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the **People's Republic of China**, including the **Hong Kong** Special Administrative Region and the **Macau Special Administrative Region**, (PRC); or the **Russian Federation** (Russia).

Automotive Manufacturers and Suppliers

Technology Providers - Suppliers of VCS hardware and software

January 16th, 2025
Publication

March 17th 2025
Entered into force

2027
Software restrictions:
Effective for model year 2027 vehicles

2030
Hardware restrictions:
Effective for model year 2030 vehicles

Essential Requirements

- Conduct supply chain audits with a precise mapping from OEM through Tier 1s and others.
- Establish comprehensive supply chain management for each contract, ensuring identification of software and hardware components based on vendor origin.
- SBOMs and HBOMs preparations to meet reporting requirements.
- Enhance compliance programs for audits and recordkeeping requirements.
- Submission of Declarations of Conformity, while maintaining supporting documentation that is readily available.

Violations & Fines

The specific maximum civil penalty will be adjusted by notice in the Federal Register effective each calendar year by the Office of the Secretary of the Department of Commerce.

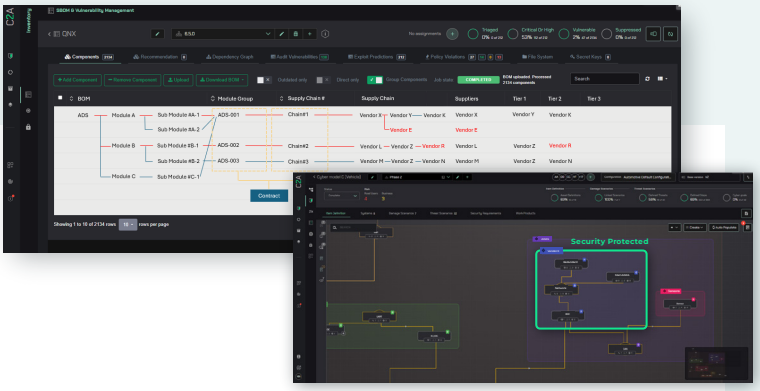
At the time of publishing of this final rule, the maximum civil penalty for violations of IEEPA is $368,136 per violation and the maximum criminal penalty is $1,000,000.

Driving Innovation with

DAIMLER TRUCK · Deloitte. · NVIDIA · BMW · APTIV · inCSS · SIEMENS · NTTGroup · MARELLI

Unmasking the DoC's Requirements

Breaking down the Essential Requirements into Common Security Practices Covered by our Product Security Platform



Supply Chain Assessment

Companies must evaluate their supply chains to ensure that Vehicle Connectivity Systems (VCS) hardware and software are not sourced from entities associated with foreign adversaries, particularly China and Russia.

Declarations of Conformity & Recordkeeping Requirements

- VCS hardware importers and connected vehicle manufacturers must submit annual or model-year Declarations of Conformity to the Bureau of Industry and Security (BIS).
- These declarations must include a HBOM or SBOM, and a list of external endpoints to which the VCS hardware connects.
- **10 years:** Maintain a full and accurate record of each transaction for which a Declaration of Conformity, general authorization, or specific authorization is."

Impact of Changing Software and the Process It Involves

- Conduct a thorough software vetting - software restrictions will impact all connected vehicle manufacturers starting in Model Year 2027.
- Identify, replace, and verify compliance of VCS software and ADS software to ensure regulatory approval.
- Software modifications will require rigorous security assessments, testing, and validation, impacting development timelines and compliance costs.

Holistic Coverage of the Rule's Requirements

C2A Security's Context-Based Risk Management & Automation Product Security Platform

Dynamic Risk Management

Stay ahead of evolving regulations with real-time risk assessment across all product security data layers, ensuring no unauthorized components enter the supply chain.
EVSec's centralized risk platform delivers continuous threat analysis, risk assessment, and management throughout the product lifecycle.

Security and Operations by Design

EVSec enables agile Product Security Development and Operations that optimizes the needed security controls for development teams and enriches operational efficiency with automated BOM updates, ensuring faster incident response and optimized security controls for development teams.

Context-based SBOM and Vulnerability Management

EVSec automates supplier compliance and regulatory monitoring while preparing SBOMs and HBOMs to meet reporting requirements, Effortlessly identify software and hardware components based on vendor origin, ensuring accurate and timely Declarations of Conformity (DoC). Continuously track supplier compliance and optimize mitigation strategies.

Supply Chain and Team Collaboration

Manage Internal Teams and the Supply Chain with EVSec, utilizing centralized real-time sharing and collaboration of systems, joint work at scale, and full visibility into the supply chain and Internal teams.
Maintain full visibility into the supply chain while ensuring audit trails for compliance actions.

On-Demand Analytics, Dashboards, and Reports

EVSec offers on-Demand analytics, dashboards, and reports that facilitate compliance workflows and data-driven decision-making.
Generate audit-ready reports aligned with ISO/SAE 21434, UN R155, BIS requirements and more.
Automate regulatory submissions and gain deep insights into risks, supply chain behavior, and business impact.

Automate Supplier Compliance and Regulatory Monitoring

Enhance **Supply Chain Visibility** with Real-Time Data

Ensure **Accurate and Documented** Declarations of Conformity

c2a-sec.com hello@c2a-sec.com

Schedule a Demo