The Clock is Ticking on EU CRA Compliance for Connected Devices

FINITE STATE

Accelerating Connected Device Security

The EU Cyber Resilience Act (CRA) sets new standards for connected device security, requiring manufacturers to implement robust cybersecurity measures across the product lifecycle, from design to end-of-life. This regulation impacts all connected devices entering the EU, mandating a fresh approach to product security and certification.

But achieving compliance doesn't have to be a burden. With Finite State's advanced analysis platform and expert services, streamline certification, enhance product security, and reduce timelines by months, ensuring you're ready for the December 11, 2027 deadline.

Act Now to Comply by 2027

Early action means...

- **Reduced Costs**
  - Avoid expensive late-stage redesigns
  - Prevent compliance-related delays
  - Optimize resource allocation
- **Competitive Advantage**
  - Early market readiness
  - Enhanced customer trust
  - Simplified supply chain management
- **Risk Mitigation**
  - Prevent certification bottlenecks
  - Ensure continuous compliance
  - Maintain market access

Accelerate Your Path to CRA Compliance with Finite State's Technology-Powered Services

Work with former government cybersecurity leaders, regulatory compliance veterans, and embedded systems specialists, and benefit from 20+ years of collective offensive security expertise.

Assessment & Strategy

- Comprehensive gap analysis
- Custom compliance roadmap
- Risk assessment & prioritization
- Security architecture review

Technical Implementation

- Automated security testing
- Supply chain verification
- Vulnerability management setup
- Monitoring implementation

Documentation & Support

- Technical documentation preparation
- CE marking guidance
- Declaration of Conformity support
- Ongoing compliance maintenance

Cut months off certification timelines • Eliminate manual processes • Prevent certification surprises • Ensure continuous compliance

Your Path Forward with Finite State

Step 1: Initial Assessment

- Evaluate current security posture
- Identify compliance gaps
- Define priority areas

Step 2: Implementation

- Deploy automated analysis
- Establish monitoring
- Begin documentation

Step 3: Ongoing Support

- Continuous compliance monitoring
- Regular security updates
- Certification maintenance

Take Action Today

The CRA represents both a challenge and an opportunity for connected device manufacturers. With Finite State's technology-powered approach and expert services, you can accelerate your path to compliance while strengthening your product security.

Don't wait until it's too late. Contact us today to learn how we can help you navigate the CRA requirements and ensure your products are ready for the European market in 2027 and beyond.

Why Choose Finite State?

> **Connected Device Expertise:** Deep understanding of IoT ecosystems and complex software supply chains.

> **Developer-Centric Workflows:** Seamless integration into existing CI/CD pipelines.

> **Comprehensive Protection:** End-to-end security across the entire product lifecycle with proprietary protocol analysis and complete visibility into your supply chain.

> **World Class Service & Support:** Our team of cybersecurity and policy experts is committed to your success.

> **Government-Grade Expertise:** Benefit from the knowledge of former senior U.S. government officials with 20+ years of cybersecurity expertise.