Future-Proofing IoT Security with the US Cyber Trust Mark

The U.S. Cyber Trust Mark is a voluntary cybersecurity labeling program designed to help consumers identify IoT devices that meet rigorous security standards.

Established by the Federal Communications Commission (FCC), the program aligns with NIST cybersecurity guidelines to enhance transparency and reduce risks associated with connected devices.

By displaying the Cyber Trust Mark, manufacturers demonstrate their commitment to strong security practices, fostering trust and resilience in the growing IoT ecosystem.

Benefits of Participation

- Improved consumer confidence in your product — *crucial for boosting sales in a crowded market*
- Positions your company as a leader in cybersecurity best practices, giving you a competitive edge
- A stronger cybersecurity posture = reduced reputational risks from security breaches
- Participation contributes to a higher standard for IoT cybersecurity across the board
- Improves internal cybersecurity practices in order to maintain certification
- Gives your organization a head start on mandatory certifications like the EU CRA

Core Requirements

Identify

Understand & manage cybersecurity risks to systems, assets, data, & capabilities.

Categories include:

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy
- Supply chain risk management

Protect

Develop & implement safeguards to ensure critical services & data are delivered securely.

Categories include:

- Identity management & access control
- Awareness & training
- Data security
- Information protection process & procedures
- Maintenance
- Protective technology

Respond

Take action when a cybersecurity event is detected to minimize its impact.

Categories include:

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

Detect

Identify cybersecurity incidents promptly.

Categories include:

- Anomalies & events
- Security continuous monitoring
- Detection processes

Recover

Restore services & operations after a cybersecurity incident.

Categories include:

- Recovery planning
- Improvements
- Communications

What Needs to be Certified

- Smart Appliances
- Fitness Trackers
- Smart Thermostats
- Baby Monitors
- Wireless Routers
- Smart Watches
- Connected Security Systems
- Voice Activated Devices
- Robot Vacuum Cleaners

Cyber Trust Mark Requirements	Finite State Solution
Compliance with NIST Cybersecurity Standards	Access a tailored regulatory compliance roadmap aligned with NIST & evolving US cybersecurity laws
Software Bill of Materials (SBOM) Transparency	Automated SBOM management throughout the SDLC, for transparency into third-party components, open-source libraries, & custom code.
Vulnerability Management & Remediation	Automated, real-time vulnerability detection in source code and binaries, enriched from 200+ threat sources.
Secure Software Development Lifecycle	Expert-led guidance for integrating security into development workflows.
Firmware & Hardware Security Validation	Outsource hardware & firmware integrity assessments to detect vulnerabilities, cryptographic weaknesses, & supply chain threats.
Testing by an Accredited, FCC-Recognized CyberLAB	Expert services to assist in the assessment of product readiness before CyberLAB submission.

Why Choose Finite State?

- **Connected Device Expertise:** Deep understanding of IoT ecosystems & complex software supply chains
- **Workflows Dev Teams Actually Use:** Seamless integration into existing CI/CD pipelines
- **Comprehensive Protection:** End-to-end security across the entire product lifecycle
- **World Class Support:** Our team of cybersecurity & policy experts is committed to your success
- **Government-Grade Expertise:** Benefit from the knowledge of former senior U.S. government officials