FINITE STATE

Ensure Compliance & Strengthen Security with Finite State

Finite State provides industry-leading cybersecurity services designed to help organizations navigate evolving regulations, enhance product security, and mitigate cyber threats. Leverage expertise from former U.S. government officials and get the support you need to tackle the evolving regulatory landscape with confidence.

IoT ● **Automotive** ● **Industrial Control Systems** ● **Healthcare**

Strategic Advisory Services

Expert guidance to align security with business and regulatory needs

- **Policy-Driven Consulting**

Leverage insights from former White House, intelligence community, and regulatory experts to shape cybersecurity policies

- **Enterprise Security Program Maturity**

Develop governance frameworks, optimize team structures, and align security operations with stakeholder needs

- **Regulatory Compliance Roadmap**

Adapt seamlessly to U.S. and EU cybersecurity regulations, including EU CRA, CE RED, and the Cyber Trust Mark

Benefits:

- Strategic alignment with evolving regulations
- Risk reduction through proactive security planning
- Tailored guidance from experienced industry professionals

Why Choose Finite State

> Deep expertise in IoT and embedded device security

> Proven track record of helping organizations meet regulatory compliance

> Comprehensive security solutions tailored to your needs

Managed Security Services

Ongoing support to maintain security posture and regulatory compliance

- **Bug Bounty Program Development**

Engage ethical hackers to uncover vulnerabilities before adversaries do

- **Virtual CPSO for IoT**

Gain expert advisory services covering technical security, compliance, and process optimization

- **Comprehensive Vulnerability & Risk Management**

Maintain security with compliance monitoring, SBOM & HBOM management, & supplier security assessments

- **Secure Software Development Lifecycle Guidance**

Integrate security into development workflows & respond swiftly to threats with expert-led guidance

Get Help Complying With...

- CE RED Article 3.3 (d)(e)(f)
- EU Cyber Resilience Act
- Connected Vehicle Regulation
- US Cyber Trust Mark
- NIST Framework
- Executive Order 14028
- FDA 524B
- CTIA Cybersecurity Certification
- AT&T & Verizon Cybersecurity Requirements

Benefits:

- Continuous threat monitoring and mitigation
- Proactive vulnerability management
- Compliance maintenance and reporting

Independent Security Validation Services

Rigorous testing to uncover vulnerabilities and ensure product security

- **Penetration Testing (IoT, ICS/OT, Healthcare, Automotive)**

Assess hardware, software, networks, APIs, and cloud infrastructure for security gaps

- **Remediation Testing & Source Code Analysis**

Validate security fixes and identify insecure coding practices, cryptographic issues, and backdoors

- **Cloud & Infrastructure Assessments**

Secure cloud deployments and critical infrastructure with targeted security evaluations

- **Hardware & Firmware Integrity & Build Reproducibility Analysis**

Identify supply chain risks and ensure binaries remain consistent across diverse build environments

Benefits:

- Uncover critical security flaws before attackers do
- Improve software and hardware security resilience
- Meet regulatory compliance with independent validation