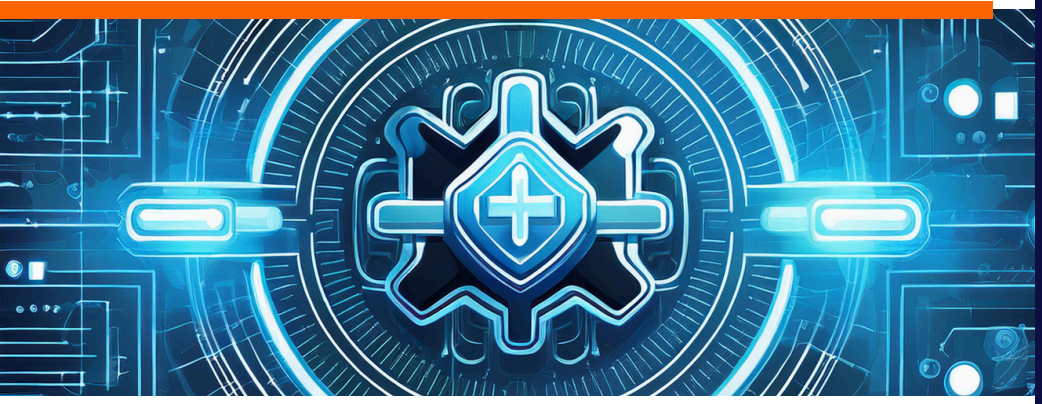
An Essential Guide to Navigating FDA Cybersecurity Compliance

FINITE STATE



The New Reality of Medical Device Security

Today, cybersecurity isn't just a technical requirement for medical devices – it's a matter of patient safety and market access. The FDA has significantly strengthened its medical device oversight, implementing stringent cybersecurity requirements that affect both new and legacy medical devices. For manufacturers, the message is clear: robust cybersecurity measures aren't optional, they're essential for market entry and maintaining compliance.

Compliance Deadline

Enforcement started October 1, 2023

Regulation Update

In March 2024, the FDA published draft guidance updates to their recommendations.

While this is still a draft, manufacturers should start aligning their premarket submissions with these recommendations.

Three Key Frameworks

Premarket Guidance

Required documentation and security measures needed *before* bringing a medical device to market. **Without premarket approval, devices cannot be legally marketed in the United States**

Based on device risk level and novelty, you need the following for premarket approval:

- 510(k) Submissions: For devices substantially equivalent to existing products
- Premarket Approval (PMA): For high-risk devices that must demonstrate safety and effectiveness through extensive data, often including clinical trials
- De Novo Requests: Novel devices without a legally marketed predicate that require a demonstration of safety and effectiveness.

Section 524B

Statutory requirements for cybersecurity device submissions

Postmarket Guidance

Ongoing security and management requirement after market entry

FDA Requirements	Finite State Solution
Cybersecurity Design Controls: *Evidence that cybersecurity has been considered in the device's design, including the implementation of necessary security features must be supplied.*	Seamless integrations into existing CI/CD pipelines ensuring that source code & compiled binaries are analyzed for security vulnerabilities early in the development process.
Software Bill of Materials (SBOM): *A detailed list of all software components, including third-party and open-source elements, to facilitate vulnerability management must be provided.*	Automated SBOM management generates SBOMs throughout the SDLC, providing comprehensive documentation on third-party components, open-source libraries, & custom code. Easily share & export documents in industry-standard formats (CycloneDX, SPDX)
Postmarket Management: *Processes to monitor, identify, and address cybersecurity vulnerabilities post-market must be established.*	Continuous monitoring and alerting for vulnerabilities ensures ongoing protection throughout a product's lifecycle. Integrated risk scoring helps teams prioritize actions by exploit and severity, while automated fixes and developer-friendly remediation recommendations fast-track necessary security fixes.
Vulnerability Management & Remediation: *Proof of vulnerability triaging must be evident in submissions.*	Automated, real-time vulnerability detection in source code and binaries helps teams identify and assess risks as they emerge, with vulnerability enrichment from 200+ threat sources.

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

> **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.