Accelerate FDA 524B Compliance for Medical Devices

RUNSAFE SECURITY'S APPROACH TO SBOM & VULNERABILITY MANAGEMENT

Medical device manufacturers face increasing regulatory scrutiny under Section 524B of the FD&C Act. An SBOM alone is not enough. The FDA expects manufacturers to demonstrate a complete, validated SBOM, a clear understanding of vulnerabilities, a risk-based remediation strategy, and a postmarket monitoring and response processes.

WHAT FDA 524B REQUIRES

524B is more than submitting an SBOM — it is demonstrating control over software risk.

SBOM	Vulnerability Management Plan	Assurance
Live, validated Software Bill of Materials (inventory only; no CVEs or remediation data).	Documented process to identify, assess, prioritize, remediate, and monitor vulnerabilities postmarket.	Evidence of secure development processes and lifecycle cybersecurity controls.

HOW RUNSAFE SUPPORTS 524B COMPLIANCE

IDENTIFY – Generate a Compliant SBOM

Complete, validated SBOM ready for FDA submission

- Build-time SBOM generation for embedded systems
- CycloneDX-compliant and aligned to NTIA minimum elements

ANALYZE – Understand Vulnerabilities & Regulatory Risk

Clear, defensible vulnerability posture to support FDA review

- Maps SBOM components to CVEs and vendor advisories
- Assesses exploitability — not just presence
- Determines urgency (patch, mitigate, monitor, accept risk)
- Supports VEX documentation

MITIGATE – Eliminate Exploitation Risk

Demonstrable risk reduction for FDA reviewers

- Makes classes of memory-based vulnerabilities non-exploitable
- Reduces risk when patches are unavailable
- No source code rewrites required

MONITOR – Support Postmarket Cybersecurity Plans

Living vulnerability management program aligned to 524B

- Continuous monitoring for new CVEs
- SBOM diff comparisons between builds
- Integration with GitHub, GitLab, Bitbucket

A STRONGER FDA 524B PACKAGE

RunSafe provides technical evidence and reporting that supports these elements.

FDA Package Component	Supported by RunSafe
SBOM	✓
Vulnerability Management Plan	✓
Threat Model & Cybersecurity Risk Assessment	✓
Secure Development Practices / Secure Product Development	✓
Postmarket Cybersecurity Plan	✓
Vulnerability Disclosure Policy / PSIRT	**
Cybersecurity Labeling / User Documentation	**

*** Subject to RunSafe customers' practice*

WHY RUNSAFE?

RunSafe helps manufacturers provide clear visibility into the software inside their products and understand which vulnerabilities create real risk. By delivering continuous insight into software components, vulnerability exposure, and product lifecycle security, RunSafe enables manufacturers to demonstrate secure product development and maintain the cybersecurity assurance required under the CRA.

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure, with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals. Learn more at: **RunSafeSecurity.com.**