Accelerate Your FDA 524B Filing with RunSafe

Generate submission-ready vulnerability assessments and documentation rapidly

RUNSAFE SECURITY

Documentation Category	Requirements / Example Content	RunSafe	RunSafe Capability/Notes
Software Bill of Materials (SBOM) Identify all software components in the device to enable vulnerability identification and response.	Machine-readable format (SPDX or CycloneDX)	✓	RunSafe generates CycloneDX compliant SBOMs
	Covers all software (OS, firmware, apps, libraries)	✓	RunSafe covers all software
	Component name, version, supplier included	✓	Reports on all mandatory NTIA minimum elements
	Unique identifiers (SPDX ID, purl, or CPE)	✓	RunSafe generates CPEs or purls
	Dependency relationships captured	✓	All software components with a full dependency tree
	Cryptographic hashes included	✓	RunSafe includes cryptographic hashes
	Tied to specific firmware/software version	✓	RunSafe generates a buildtiime SBOM so it is created when firmware or software image is produced
	Generated by tooling (not manually compiled)	✓	Automates SBOM generation as part of ever software pipeline's build
Vulnerability Management Plan Describe how the manufacturer identifies, assesses, prioritizes, and remediates cybersecurity vulnerabilities throughout the device lifecycle.	Vulnerability intake sources (NVD, vendor advisories, internal testing)	✓	RunSafe incorporates dozens of sources (including NVD and vendor advisors) to identify vulnerabilities associated with each component of an SBOM
	Monitoring frequency and tools	✓	RunSafe monitors for new alerts on a frequency determined by user and allows to compare for diffs between builds
	Severity/impact assessment (CVSS + patient safety impact) NOTE: vulnerability should be mapped to SBOM component ID	✓	Risk Reduction Analysis tool analyzes exposure to CVEs and potential zero days; and determines if a vuln is exploitable
	Remediation decision criteria (patch, mitigation, risk acceptance)	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon). RS Protect makes vulnerability non-exploitable.
	Remediation timelines by severity	✓	RunSafe eliminates exploitation of entire classes of vulns even when a patch is not available
	Patch verification and validation approach	✓	RunSafe identifies the version where patching is needed, and users can triage patches; also RunSafe confirms when a vulnerability is not exploitable
Threat Model & Cybersecurity Risk Assessment Demonstrate understanding of potential cybersecurity threats and their impact on device safety and effectiveness.	System architecture and data flow description		Subject to RunSafe customers' practices
	Trust boundaries and attack surfaces		Subject to RunSafe customers' practices
	Threat modeling methodology (e.g., STRIDE)		Subject to RunSafe customers' practices
	Identified threats and misuse cases	✓	Risk Reduction Analysis tool analyzes exposure to CVEs and memory-based zero days
	Risk scoring (likelihood × impact)	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon).
	Mitigations and residual risk justification	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon). RS Protect makes vulnerability non-exploitable.
Secure Development Practices / Secure Product Development Show that cybersecurity is integrated into the product's design and development lifecycle	Secure software development lifecycle activities	✓	RunSafe enforces policies at build time so customers do not release code violating a regulatory control or company governance policy
	Secure coding standards and code review practices		Subject to RunSafe customers' practices
	Static and dynamic analysis processes		Subject to RunSafe customers' practices
	Third-party and open-source software controls	✓	RunSafe captures data on open source repos and risk related to open-source software controls
	Build environment and artifact integrity controls	✓	RunSafe captures artifacts generated by compiler at build time to include in SBOM
	Release and change management processes		Subject to RunSafe customers' practices
Postmarket Cybersecurity Plan Explain how cybersecurity risks are monitored and managed after the device is released to the market.	Ongoing vulnerability monitoring process	✓	Supports VEX to communicate known, specific vulnerabilities
	Field issue intake and triage	✓	RunSafe allows users to identify issues and triage; directly with RunSafe Identify or within issue managers in GitLab, GitHub, BitBucket and more
	Incident response and escalation procedures		Subject to RunSafe customers' practices
	Clinical and safety impact assessment		Subject to RunSafe customers' practices
	Secure update and patch deployment process	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon).
	Regulatory reporting criteria and timelines	✓	RunSafe has on demand reports to support regulatory submissions.
Vulnerability Disclosure Policy / PSIRT Provide a mechanism for external parties to responsibly report cybersecurity vulnerabilities.	Vulnerability reporting channels		Subject to RunSafe customers' practices
	Acknowledgment and response timelines		Subject to RunSafe customers' practices
	Investigation and coordination process	✓	Incorporate RunSafe in the vulnerability investigation process. RunSafe incorporate sources to identify vulnerabilities with the SBOM, monitors for new alerts, andanalyzes exposure to CVEs and potential zero days; and determines if exploitable
	CVE request and assignment handling		Subject to RunSafe customers' practices
	Responsible disclosure timelines		Subject to RunSafe customers' practices
	Public advisory issuance criteria		Subject to RunSafe customers' practices
Cybersecurity Labeling / User Documentation Inform users how to deploy, configure, and maintain the device securely.	Intended use environment assumptions		Subject to RunSafe customers' practices
	Cybersecurity features and controls described		Subject to RunSafe customers' practices
	User configuration and maintenance responsibilities		Subject to RunSafe customers' practices
	Update and patch instructions provided		Subject to RunSafe customers' instructions for updates/patches
	Logging/monitoring guidance (eg how to access logs)		Subject to RunSafe customers' practices
	Known cybersecurity limitations disclosed		Subject to RunSafe customers' practices