



GUIDE

FDA Cybersecurity Deficiency Letter Response Checklist

Free Resource · Updated 2026 FDA Cybersecurity Deficiency Letter Response Checklist A step-by-step, 11-stage checklist for organizing and resolving your FDA cybersecurity deficiency for 510(k), PMA,

Free Resource · Updated 2026 FDA Cybersecurity Deficiency Letter Response Checklist A step-by-step, 11-stage checklist for organizing and resolving your FDA cybersecurity deficiency for 510(k), PMA, De Novo, and HDE submissions. Aligned with the FDA's February 2026 final guidance and Section 524B o

How to Use This Checklist

When you receive an FDA cybersecurity deficiency letter (also called an Additional Information request or Major Deficiency), work through each step in order and check off items as you complete them.

This checklist aligns with the FDA's February 2026 final guidance, *Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions*, and Section 524B of the FD&C Act. Not sure where to start? Schedule a no-cost discovery call →

- 11 - Actionable Steps (From triage to final submission)
- 9 - Standards Referenced (FDA-aligned frameworks)
- 60-90 - Days Typical Timeline (From receipt to resubmission)

11 Steps to a Complete FDA Cybersecurity Response

Work through each step in order. Every checklist item maps directly to a requirement in the FDA's February 2026 guidance or Section 524B. If you need help with any step, our team is one call away.

Initial Assessment & Triage

- Read the deficiency letter in full and identify every discrete finding
- Categorize each deficiency by the relevant 524B subsection:
 - 524B(b)(1): Postmarket monitoring, patching plans, and CVD procedures
 - 524B(b)(2): SPDF and processes for reasonable assurance of cybersecurity
 - 524B(b)(3): Software Bill of Materials (SBOM)
- Determine submission type (510(k), PMA, De Novo, HDE, PDP, or BLA)
- Confirm device meets the "cyber device" definition under Section 524B(c)



- Note the FDA reviewer name, division, and submission number
- Record the response deadline or target resubmission date

Threat Modeling

- Perform or update threat modeling per FDA guidance (Section V.A.1)
- Identify all medical device system risks and mitigations
- State assumptions about the environment of use (e.g., hostile network)
- Capture supply chain, manufacturing, deployment, and decommission risks
- Ensure threat model covers the full medical device system end-to-end
- Map each threat to a specific mitigation or risk control measure
- Align with AAMI TIR57 / ANSI/AAMI SW96 or equivalent framework
- Provide rationale for the threat modeling methodology selected

Cybersecurity Risk Assessment

- Perform a security risk assessment separate from the safety risk assessment
- Assess exploitability of identified vulnerabilities (not probabilistic)
- Capture pre- and post-mitigation risk scores and acceptance criteria
- Document residual risk conclusions with clinical justification
- Cross-reference CISA Known Exploited Vulnerabilities Catalog
- Ensure security risks are traced into the safety risk process (ISO 14971)
- Provide traceability between threat model, risk assessment, and SBOM

SBOM (Software Bill of Materials)

- Generate or update SBOM in machine-readable format (SPDX or CycloneDX)
- Provide both machine-readable (JSON/XML) and human-readable versions
- Include NTIA minimum elements for each component:
 - Supplier name, component name, version, unique identifiers, dependency relationships, SBOM author, timestamp
- Known vulnerabilities mapped per component (CVE status)
- List all third-party, open-source, and off-the-shelf (OTS) components
- Include support end dates and known vulnerabilities for each component
- Flag end-of-life components with risk rationale or replacement plan



- Verify SBOM completeness against binary SCA and build system

Security Architecture & Design Controls

- Provide architecture views: global system, multi-patient harm, updateability, security use cases
- Include interface diagrams, trust boundaries, and data flow documentation
- Document authentication and access control mechanisms
- Describe cryptographic implementations (at rest and in transit)
- Detail secure boot and firmware/code integrity verification
- Document event detection, logging, and anomaly detection
- Describe resiliency and recovery mechanisms
- Document firmware and software update mechanisms (Appendix 1.H)

Cybersecurity Testing

- Verify security requirements testing: each input mapped to implementation
- Provide threat mitigation testing per each architecture view
- Perform vulnerability testing per ANSI/ISA 62443-4-1:
- Abuse/misuse cases and malformed/unexpected inputs
- Robustness and fuzz testing
- Attack surface analysis
- Vulnerability chaining assessment
- Closed-box known vulnerability scanning
- Software composition analysis of binary executables
- Static and dynamic code analysis (SAST), including hardcoded credentials
- Perform penetration testing and include in report:
- Independence and expertise of testers
- Scope and duration of testing
- Methods employed, results, findings, and observations
- Map all findings to threat model with remediation or formal risk acceptance
- Retest after remediations to confirm fixes are effective
- Assess unresolved anomalies for security impact (including CWE categories)



SPDF & Quality Management System Integration

- Document your Secure Product Development Framework (SPDF) per 524B(b)(2)
- Integrate SPDF into the QMSR (21 CFR 820) and ISO 13485 processes
- Ensure traceability from threat model to risk management file
- Connect cybersecurity design controls to your design history file (7.3.10)
- Verify cybersecurity activities are tied to change management (ECO process)
- Document custodial control of source code (escrow or backup for OTS)
- Include plans for replacing third-party components at end-of-support

Postmarket & Vulnerability Management Plan

- Define specific monitoring sources (NVD, ICS-CERT / CISA, vendor advisories)
- Define vulnerability response timelines based on severity and clinical risk
- Include justifications for response timelines and any deviations
- Name responsible roles and escalation paths for vulnerability response
- Document coordinated vulnerability disclosure (CVD) procedures per 524B(b)(1)
- Describe patch delivery and software update mechanisms
- Detail how updates are authenticated and verified on the device
- Describe rollback capabilities if an update fails
- Account for both currently marketed and fielded legacy devices
- Track and report defect density, time-to-patch, and deployment metrics
- Confirm monitoring processes and tooling are operational before market entry. See our postmarket services →

Cybersecurity Labeling & Transparency

- Include cybersecurity information in device labeling per Section 502(f)
- Disclose all communication interfaces and third-party software in labeling
- Provide users with information to securely configure and update the device
- Document known vulnerabilities and risk information for end users
- Include risk transfer information and any user-required security actions

Response Document Preparation

- Draft a point-by-point response to each deficiency item



- Cross-reference responses with updated technical documentation
- Include all supporting evidence: test reports, SBOM, SPDF, architecture views
- Have a regulatory affairs specialist review the response language
- Verify response format meets FDA eSTAR or eCopy requirements
- Confirm section mapping against current FDA submission template
- Conduct an internal review or dry run before submission

Final Submission & Follow-Up

- Submit response via the appropriate FDA portal
- Retain a complete copy of all submitted materials
- Set a follow-up reminder for FDA response (typically 60-90 days)
- Prepare for potential interactive review or follow-up questions
- Verify postmarket monitoring processes are live before device reaches market
- Document lessons learned for future submissions

| Need Expert Help With Your FDA Response?

Blue Goat Cyber focuses exclusively on medical device cybersecurity. Every engagement is structured around FDA clearance - we don't handle enterprise IT. When you work with us on a deficiency response, you get a team that has written the artifacts, argued the cases, and gotten devices cleared.

Schedule a Discovery Session

Or explore all medical device cybersecurity services →

Our Promise

We respond within 24 hours with a quote.

Tell us about your device, your timeline, and your submission type. No sales pressure - just a clear, honest assessment and a fixed-price quote.

This checklist is provided free of charge by Blue Goat Cyber. It is informational and does not constitute legal or regulatory advice. bluegoatcyber.com · (844) 939-4628

Ready to talk through your roadmap?

[Book a Strategy Session](#) →

Source guide: [fda-cybersecurity-deficiency-response-checklist](#). For the most current version, visit bluegoatcyber.com/guides/fda-



[cybersecurity-deficiency-response-checklist.](#)