BLUE GOAT CYBER

Medical Device Cybersecurity · FDA Specialists

FDA CYBERSECURITY DEFICIENCY RESPONSE CHECKLIST

FDA Cybersecurity Deficiency Letter Response Checklist

A step-by-step, 11-stage checklist for organizing and resolving FDA cybersecurity deficiencies across 510(k), PMA, De Novo, and HDE submissions.

© Blue Goat Cyber. For educational use. Not legal or regulatory advice.

WHY THIS MATTERS

Which letter did the FDA send you?

Response strategy, review clock, and submission mechanics differ for each letter type. This checklist aligns to the FDA February 2026 Final Premarket Cybersecurity Guidance and Section 524B of the FD&C Act: 11 actionable steps, 9 standards referenced, and a 60-90 day typical response timeline.

Key takeaway: Answer the letter you actually received. An AI letter is a submission amendment against a paused 180-day clock; an RTA means the submission never entered substantive review. Filing the wrong artifact restarts the review instead of closing it.

- **Additional Information (AI) Letter / AINN.** Most common cybersecurity finding. Review clock pauses; you have 180 days to submit a complete response or the submission is withdrawn. File as a submission amendment, not a new 510(k).
- **Major Deficiency Letter (PMA / De Novo).** Substantive scientific or technical issues. Same 180-day clock; every item is a hold on clearance until resolved.
- **Hold Letter.** The FDA needs information before substantive review can continue (PMA path). Clock pauses; address every hold item before review resumes.
- **Refuse to Accept (RTA) - 510(k).** Issued in the first 15 days when the submission fails the acceptance checklist (commonly missing SBOM, threat model, or 524B element). 180 days to fix and resubmit via eSTAR; submission has not yet entered substantive review.
- **Refuse to Accept (RTA) - De Novo.** Same mechanic against the De Novo acceptance checklist.

Standards referenced in this checklist

ISO 14971 · ANSI/AAMI SW96 · AAMI TIR97 · IEC 62304 · IEC 81001-5-1 · IEC 62443-4-1 · ISO 13485 · UL 2900 · NIST SP 800-115

11 steps to a complete FDA cybersecurity response

Work through each step in order. Every checklist item maps to a requirement in the FDA February 2026 guidance or Section 524B.

STEP 01

Initial assessment and triage

- Read the deficiency letter in full and identify every discrete finding.
- Categorize each deficiency by 524B(b)(1) postmarket / 524B(b)(2) SPDF / 524B(b)(3) SBOM.
- Determine submission type - 510(k), PMA, De Novo, HDE, PDP, or BLA.
- Confirm the device meets the cyber device definition under Section 524B(c).
- Record reviewer name, division, submission number, and response deadline.

STEP 02

Threat modeling

- 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.
- Cover the full medical device system end-to-end.
- Map each threat to a specific mitigation or risk control.
- Align with ANSI/AAMI SW96:2023 or equivalent.
- Provide rationale for the threat modeling methodology selected.

STEP 03

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 with clinical justification.
- Cross-reference the CISA Known Exploited Vulnerabilities Catalog.
- Trace security risks into the safety risk process (ISO 14971).
- Provide traceability between threat model, risk assessment, and SBOM.

STEP 04

SBOM (Software Bill of Materials)

- Generate SBOM in machine-readable format (SPDX or CycloneDX).
- Provide both machine-readable (JSON/XML) and human-readable versions.
- Include NTIA minimum elements per component: supplier, name, version, unique IDs, dependency relationships, SBOM author, timestamp.
- List all third-party, open-source, and OTS components with known CVEs.
- Include support end dates and EOL components with risk rationale or replacement plan.
- Provide a VEX (Vulnerability Exploitability eXchange) document for every component with known CVEs - status: not affected, affected, fixed, or under investigation, with justification.
- Verify SBOM completeness against binary SCA and build system.

STEP 05

Security architecture and 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).

STEP 06

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, robustness/fuzz, attack surface, vulnerability chaining, closed-box known-vuln scanning, binary SCA, SAST/DAST including hardcoded credentials.
- Perform penetration testing and include independence/expertise of testers, scope, duration, methods, results, findings.
- Map all findings to threat model with remediation or formal risk acceptance.
- Retest after remediation. Assess unresolved anomalies for security impact (including CWE categories).

STEP 07

SPDF and QMS integration

- Document your Secure Product Development Framework (SPDF) per 524B(b)(2).
- Integrate SPDF into 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).
- Tie cybersecurity activities 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.

STEP 08

Postmarket and vulnerability management plan

- Define specific monitoring sources (NVD, ICS-CERT / CISA, vendor advisories).
- Define vulnerability response timelines by severity and clinical risk, with justification.
- Name responsible roles and escalation paths.
- Document coordinated vulnerability disclosure (CVD) procedures per 524B(b)(1).
- Describe patch delivery, update authentication, and rollback if an update fails.
- Account for both currently marketed and fielded legacy medical devices.
- Track and report defect density, time-to-patch, and deployment metrics.
- Confirm monitoring processes and tooling are operational before market entry.

STEP 09

Cybersecurity labeling and 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.

STEP 10

Response document preparation

- Draft a point-by-point response - quote the FDA's exact wording first, then your response.
- Write a cover letter listing every deficiency by number, your one-line resolution, and the section/page where the FDA will find the new evidence.
- Cross-reference responses with updated technical documentation.
- Include all supporting evidence: test reports, SBOM, SPDF, architecture views.
- Include a traceability matrix mapping every deficiency item to response section to updated artifact (file name + version).
- Have a regulatory affairs specialist review the response language.
- Verify response format meets FDA eSTAR or eCopy requirements.
- Confirm section mapping against the current FDA submission template.
- Conduct an internal review or dry run before submission.

STEP 11

Final submission and follow-up

- Submit via the appropriate FDA portal - eSTAR for 510(k); CDRH Portal for PMA/De Novo amendments.
- Submit as a submission amendment (responding to an AI letter / hold) - do not file a new 510(k) or supplement unless explicitly directed.
- Confirm you are well within the 180-day response clock (Day 1 = date on the AI letter); request a written extension before the clock expires if needed.
- Retain a complete copy of all submitted materials with version-controlled file names.
- Set a follow-up reminder for FDA response (typically 60-90 days).
- Prepare for interactive review or follow-up questions; assign a single point of contact who can respond within 5 business days.
- Verify postmarket monitoring processes are live before the device reaches market.
- Document lessons learned for future submissions.

WORK WITH US

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.

- Deficiency letter analysis and response strategy
- Threat modeling and SPDF documentation
- SBOM generation, VEX, and vulnerability assessment
- Penetration testing (FDA-ready reports)
- Full 524B submission support and review
- Postmarket cybersecurity management

Our commitment

Send us your FDA letter and we'll deliver a free written gap analysis within 24 hours, followed by a fixed-fee quote. No sales pressure - just a clear, honest assessment.

Schedule a discovery session: bluegoatcyber.com/contact

Full guide online: bluegoatcyber.com/guides/fda-cybersecurity-deficiency-response-checklist

This checklist is provided free of charge by Blue Goat Cyber. It is informational and does not constitute legal or regulatory advice.