BLUE GOAT CYBER
Medical Device Cybersecurity

CHECKLIST

FDA Cybersecurity Deficiency Letter Response Checklist

An 11-stage checklist for organizing and resolving FDA cybersecurity deficiency letters across 510(k), PMA, De Novo, and HDE submissions.

Reviewed 2026-10-18

Book a free discovery call
30 minutes with a senior expert
bluegoatcyber.com/discovery-call

IN BRIEF

Respond to an FDA cybersecurity deficiency letter as a submission amendment (never a new 510(k) or a supplement), within 180 calendar days of a 510(k) AI request; for other pathways, follow the letter and applicable regulation. Answer every finding point by point, quoting the reviewer's wording verbatim, and attach the updated artifact that closes it: threat model, security risk assessment, SBOM with optional VEX, architecture views, retest report, SPDF narrative, or labeling. The 11 steps below work the letter from triage to resubmission.

Talk to a deficiency expert · Our response service · Download the printable PDF checklist

This checklist covers **510(k), PMA, De Novo, and HDE submissions** and is aligned with the FDA's February 2026 final guidance and Section 524B of the FD&C Act (21 U.S.C. 360n-2).

Which Letter Did the FDA Send You?

Identify the letter type before you draft a word. Response strategy, clock, portal, and submission mechanics all differ.

Letter type	Where you are in review	Your clock	How you respond	What closes it
Additional Information (AI) letter / AINN - 510(k)	Substantive review, clock paused	180 calendar days from the date of the letter	Submission amendment through eSTAR	Point-by-point response with the updated artifact attached for every finding
Major deficiency letter (PMA / De Novo)	Substantive review, clock paused	Deadline in the letter and applicable regulation	Amendment through the CDRH Customer Collaboration Portal	Evidence for each item, often paired with a meeting request
Hold letter (PMA)	Review suspended pending information	Stated in the letter and applicable PMA regulation	Amendment to the pending application	Every hold item addressed with objective evidence
Refuse to Accept (RTA) - 510(k)	Acceptance screen, before substantive review (the FDA issues the RTA decision within 15 calendar days of receipt)	180 calendar days to submit a complete response	Corrected submission reuploaded through eSTAR under the same submission number	The missing acceptance-checklist item supplied in full (commonly SBOM, threat model, or a 524B element)
Refuse to Accept (RTA) - De Novo	Acceptance screen	180 calendar days	Corrected De Novo submission	Same mechanic as 510(k) RTA, against the De Novo acceptance checklist

Two things people get wrong on this table. First, the 15 days on the RTA row is the FDA's window to issue the decision, not your window to respond; the 180-calendar-day rule applies to 510(k) AI and acceptance-hold responses; other pathways follow their letter and applicable regulation. Second, an AI response is an **amendment** to the pending submission. A supplement is a separate regulatory action against an already-cleared or approved device, and filing one in response to an AI letter creates a new submission and a new fee.

If your letter cites Section 524B, AAMI TIR57, ANSI/AAMI SW96:2023, or the FDA February 2026 final premarket cybersecurity guidance, the rest of this checklist applies directly. Not sure which type you received? Send us the letter and we'll triage it free →

Where this guide sits in the cluster. This page is the process: what to do, in order, once the letter is in hand. If you want to see real reviewer wording and worked responses, read deficiency letter examples and analysis. If you need to schedule the rebuild work inside the 180-day clock, read FDA cybersecurity deficiency response timeline and sequencing. If you want the root causes to avoid next time, read what triggers FDA cybersecurity deficiencies. For a ranked share of what 30+ FDA letters raised most, see our Top FDA Cybersecurity Deficiencies report. For the letter-type distinction alone, see deficiency vs RTA vs hold. If you would rather hand the whole cycle to a team that does this weekly, that is our FDA Cybersecurity Deficiency Response service.

How to Use This Checklist

Work the 11 steps in order and check items off as you complete them. Steps 2 through 9 describe recommended evidence to select according to the letter and device risks; Steps 1, 10, and 11 are triage, assembly, and submission mechanics.

Each item maps to the FDA's February 2026 final guidance, Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions, or to Section 524B of the FD&C Act (21 U.S.C. 360n-2). Not sure where to start? Schedule a no-cost discovery call →

Standards referenced in this checklist:

- ISO 14971 (safety risk management)
- AAMI TIR57 / ANSI/AAMI SW96:2023 (security risk management)
- ANSI/AAMI SW96 (medical device security risk management)
- IEC 62304 (medical device software lifecycle)
- IEC 81001-5-1 (health software security activities)
- IEC 62443-4-1 (secure product development)
- ISO 13485 (medical device QMS)
- UL 2900 (software cybersecurity for network-connectable products)
- NIST SP 800-115 (technical security testing)

Also see our companion guide: The MedTech Cybersecurity Standards Decoder →

At a glance: 11 actionable steps · **9** standards referenced · **60-90** days typical timeline from receipt to resubmission.

11 Steps to a Complete FDA Cybersecurity Response

Work through each step in order. Checklist items combine recommended evidence with applicable statutory obligations and should be scoped to the actual findings; they are not all requirements in the FDA's February 2026 guidance or to Section 524B of the FD&C Act (21 U.S.C. 360n-2). If you need help with any step, our team is one call away.

Step 1 · 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 plan and CVD procedures
- 524B(b)(2): SPDF processes for reasonable assurance of cybersecurity, plus postmarket updates and patches
- 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

Step 2 · 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

Step 3 · Cybersecurity Risk Assessment

- ✓ Make the security risk assessment identifiable and traceable to safety risk analysis; a separate file is recommended packaging, not mandatory
- ✓ 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

Step 4 · 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 (superseded by CISA's 2026 Minimum Elements for an SBOM, published July 29, 2026) 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
- ✓ Provide a **VEX (Vulnerability Exploitability eXchange)** document for every component with known CVEs - state whether each CVE is exploitable in your device's deployed configuration (status: not affected, affected, fixed, under investigation) with justification
- ✓ Verify SBOM completeness against binary SCA and build system

Step 5 · 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)

Step 6 · 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)

Step 7 · 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

Step 8 · 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 →

Step 9 · 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

Step 10 · Response Document Preparation

- ✓ Draft a point-by-point response to each deficiency item - quote the FDA's exact wording first, then your response
- ✓ Write a **cover letter** that lists 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 → response section → 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 current FDA submission template
- ✓ Conduct an internal review or dry run before submission

Step 11 · Final Submission & Follow-Up

- ✓ Submit response 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 the FDA explicitly directs you to
- ✓ For a 510(k) AI request, provide a complete response within **180 calendar days** or the submission is considered withdrawn; do not assume an extension is available. Other pathways follow the letter and applicable regulation
- ✓ 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 potential 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 device reaches market

- ✓ Document lessons learned for future submissions

What Reviewer Language Actually Looks Like, and How to Answer It

Deficiency items follow a predictable shape: a statement of what the FDA could not find, a citation to the guidance section or statute, and a request for specific information. Below are paraphrased versions of recurring cybersecurity items and the response structure that closes each one. (For full worked examples with the surrounding letter context, see deficiency letter examples and analysis.)

What the reviewer typically writes	What they are actually asking for	What closes it
"The threat model provided does not appear to address the full medical device system, including the cloud infrastructure and companion mobile application."	Scope, not depth. The model stopped at the device boundary.	Reissued threat model covering every trust boundary end to end, with a revision history line stating what was added
"It is unclear how the security risk assessment relates to the safety risk analysis provided under ISO 14971."	The traceability link between security and safety risk.	Traceability table mapping each threat to its security risk ID and the corresponding ISO 14971 hazard, plus the updated risk management file section
"Please provide a Software Bill of Materials that includes the level of support provided by each component's manufacturer and the end-of-support date."	Missing NTIA/CISA metadata fields, not a missing SBOM.	Regenerated machine-readable SBOM with support level and end-of-support columns populated, plus an optional VEX document for open CVEs
"The penetration testing report does not describe the independence and technical qualifications of the testers, nor the scope and duration of testing."	Report methodology sections, not more testing.	Revised report with an independence statement, tester qualifications, scope statement with explicit exclusions, dates, and hours
"Please provide justification for the proposed vulnerability response timelines."	Rationale tied to clinical risk, not a generic SLA table.	Revised postmarket plan with severity tiers, the clinical-risk reasoning behind each timeline, and the deviation process

Response wording that works

Use the same three-part structure for every item. Restate, answer, point to the evidence.

FDA Deficiency 3: "Please provide a Software Bill of Materials that includes the level of support provided by each component's manufacturer and the end-of-support date." **Response:** A revised SBOM has been generated in CycloneDX 1.6 format and is provided as Attachment 3-A (SBOM_DeviceName_v2.1.json), with the human-readable equivalent in Attachment 3-B. Each of the 148 components now includes supplier name, version, unique identifier, dependency relationship, support level, and end-of-support date. Twelve components with published CVEs are addressed in the accompanying VEX document (Attachment 3-C), which states exploitability status and justification for each. Section 8.3 of the updated Cybersecurity Management Plan (Attachment 3-D, revision C) describes the regeneration procedure and monitoring

cadence. No change to device design was required to close this item.

Three rules behind that wording. Quote the deficiency verbatim so the reviewer does not have to match your paragraph to their letter. Name the attachment, file name, and revision for every claim. State plainly whether the device design changed, because that is the reviewer's next question.

Avoid the two responses that reliably fail: arguing the finding away without new evidence, and promising a future artifact ("will be completed prior to launch") where the guidance expects one at submission.

How Blue Goat Cyber Approaches FDA Cybersecurity Deficiency Response

Deficiency response is where most submissions stall - or die. We run it as a focused engagement with an agreed scope and schedule; the FDA decides whether the response is adequate. Here is the model.

- **24-hour quote and triage support.** We categorize every deficiency (RTA, AI, Major, Minor), map it to controlling FDA guidance, and identify which findings need remediation vs. explanation vs. new evidence.
- **Original submission audit.** Before responding we re-read what you shipped. Check traceability across the evidence package.
- **Evidence, not narrative.** Reviewers want documents (threat model updates, retest reports, updated SBOMs, revised SPDF plans) - not a cover letter arguing the finding away. We produce those documents.
- **Q-Sub when it saves a cycle.** For ambiguous deficiencies we scope a pre-response Q-Sub so you get FDA alignment before spending 90 days on the wrong fix.
- **Response package assembled the way FDA reads it.** Each deficiency answered in order, with cross-references and the underlying artifact attached.
- **Agreed scope and schedule.** Confirm engineering, device-access, approval, and retesting dependencies against the actual deadline. If the FDA raises a cybersecurity question, we answer it at no extra cost until the cybersecurity portion is closed.

Our FDA Cybersecurity Deficiency Response engagement is the entry point.

Frequently asked questions

How long do we have to respond to an FDA cybersecurity deficiency letter?

For a 510(k) Additional Information (AI) letter you have 180 calendar days from the date on the letter. Miss that window and the submission is withdrawn and you file (and pay) again. Deficiencies inside a De Novo or PMA follow the pathway-specific hold and interactive review clocks, but the practical target is the same: respond within 60 to 90 days to keep the reviewer engaged.

Can we respond partially and defer the rest?

You can, but it is a bad idea. Reviewers treat a partial response as a signal that the manufacturer has not internalized the deficiency, which usually produces a second, broader deficiency letter. Fully answer every item in the letter in one submission, even if some items require you to acknowledge open work with a dated remediation plan.

Should we schedule a Q-Sub before responding?

Only if the letter contains an ambiguous item where the FDA's expectation is genuinely unclear. A Q-Sub adds three to four months to the timeline and is rarely worth it for a routine cybersecurity deficiency where the guidance is prescriptive. Reserve Q-Subs for novel devices, first-in-class cybersecurity questions, or when a reviewer explicitly invites one.

Do we need to redo the pen test if the FDA cites test coverage?

Usually yes, at least partially. A deficiency that cites incomplete pen test scope, missing attack vectors, or shallow testing rarely closes with a narrative response. Rescope with the specific gaps the reviewer named, run the incremental testing, and attach the revised report. Reusing the original report with a cover letter almost never clears the deficiency.

What is the difference between an AI letter, an RTA hold, and a "major deficiency"?

RTA is an acceptance screen: the FDA issues the decision within 15 calendar days of receipt, before substantive review starts, and you have 180 days to submit a complete corrected submission. An AI letter comes during substantive review, pauses the review clock, and also gives you 180 calendar days from the date of the letter. "Major deficiency" is the language reviewers use, mainly on PMA and De Novo, for items that would prevent approval if unresolved. All three require a written response, and in every case the response is an amendment to the pending submission rather than a new one.

Does responding to a cybersecurity deficiency require a new predicate analysis?

Not usually. Cybersecurity deficiencies typically live in the substantive review of the cybersecurity subform and do not touch substantial equivalence. The exception is when the reviewer questions whether cybersecurity differences between your device and the predicate raise a new safety and effectiveness question. Then predicate analysis becomes part of the response.

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 & Response Strategy
- Threat Modeling & SPDF Documentation
- SBOM Generation & Vulnerability Assessment
- Penetration Testing (Reports for FDA Premarket Submissions)

- Full 524B Submission Support & Review
- Postmarket Cybersecurity Management

Schedule a Discovery Session

Or explore all medical device cybersecurity services →

This checklist is informational and does not constitute legal or regulatory advice.

Need help working the checklist on a live FDA letter? Our FDA Cybersecurity Deficiency Response service is scoped to answer every item in one resubmission, with a fixed fee and an NDA in place before you send anything. We provide 24-hour quote and triage support; a complete written analysis and remediation schedule are separately scoped.

See also: Deficiency letter examples & analysis · Top FDA Cybersecurity Deficiencies report · Deficiency vs RTA vs Hold letter · What triggers FDA cybersecurity deficiencies

Free tools for this

- FDA Deficiency Letter Triage - classify each deficiency and plan the response order.

Current web guide: bluegoatcyber.com/guides/fda-cybersecurity-deficiency-response-checklist

Talk to a senior medical device cybersecurity expert

Book a free 30-minute discovery call. Scan the code or visit bluegoatcyber.com/discovery-call. You get a written quote within 24 hours.

Informational material. Confirm requirements for your device and market. The manufacturer owns risk decisions, QMS approvals, and regulatory submissions. No regulatory outcome is promised.