



GUIDE

12 Reasons the FDA Rejects Medical Device Cybersecurity Submissions

The 12 most common cybersecurity deficiencies in 510(k), De Novo, and PMA submissions - what triggers each one, and exactly how to fix it before you submit.

A practical, ungated guide to the most common cybersecurity deficiencies in 510(k), De Novo, and PMA submissions - what triggers each one, and exactly how to fix it before you submit.

By the numbers: 250+ submissions cleared · 0 FDA rejections · 12 common deficiencies · 24-hour fixed-fee quote · 8-12 weeks added to clearance per AI letter on cybersecurity.

Why cybersecurity is now the #1 hold on premarket clearance

Since Section 524B of the FD&C Act took effect, FDA has explicit authority to refuse to accept any premarket submission for a cyber device that doesn't meet cybersecurity requirements. With FDA's Feb 3, 2026 final guidance now in force, and the Quality Management System Regulation (QMSR, 21 CFR Part 820) incorporating ISO 13485:2016 effective February 2, 2026, submissions that would have sailed through three years ago are now routinely held for cyber deficiencies - and an AI letter on cybersecurity can add months to your clearance timeline.

The patterns are predictable. After 250+ submissions with zero rejections, we see the same twelve issues come up again and again. This guide walks through each one: what reviewers see, why it's flagged, and exactly how to fix it before you submit.

FDA alignment: Every recommendation in this guide is aligned to FDA's current final guidance, Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions (Feb 3, 2026), and to Section 524B of the FD&C Act.

How to use this guide

- Read each reason as a self-assessment: do you have the artifact, and is it at the depth FDA expects?
- Use the checklist at the end to score your submission readiness.
- Where you find a gap, the fix list is concrete enough to start work on Monday.

What FDA flags - and how to fix it before you submit

Each deficiency below is drawn from real submission cycles. An AI letter on any one of these can add 8-12 weeks to your clearance timeline.



1. Incomplete or shallow Software Bill of Materials (SBOM)

Category: SBOM / third-party components

What reviewers see. Submission includes a high-level component list but is missing transitive dependencies, version pins, supplier identifiers, or a recognized format (SPDX / CycloneDX).

Why it's flagged. FDA requires a machine-readable SBOM that supports vulnerability monitoring across the entire device lifecycle - not a static spreadsheet snapshot. Reviewers will issue a deficiency if they can't trace third-party components or evaluate known vulnerabilities.

How to fix it.

- Generate the SBOM in CycloneDX or SPDX format directly from your build pipeline.
- Include all transitive dependencies, exact versions, suppliers, and license data.
- Document the SBOM maintenance process: how it's regenerated on each release and how vulnerabilities are tracked against it post-market.

2. Threat model not aligned to AAMI TIR57 or FDA expectations

Category: Threat modeling

What reviewers see. Threat model is generic, lacks data flow diagrams with trust boundaries, or doesn't connect identified threats to security controls and risk acceptance.

Why it's flagged. FDA expects threat modeling that explicitly links assets, threats, vulnerabilities, and controls to patient safety risk. A STRIDE table without context or traceability rarely passes review.

How to fix it.

- Build data flow diagrams that show every interface, trust boundary, and external entity.
- Use a recognized methodology (STRIDE, PASTA) and tie each threat to a control or risk acceptance.
- Cross-reference threats with the Security Risk Assessment and ISO 14971 risk file.

3. Security Risk Assessment not integrated with ISO 14971

Category: Risk management

What reviewers see. Cybersecurity risks are tracked in a separate document with no link to the device's safety risk management file.

Why it's flagged. FDA's premarket guidance is explicit: cybersecurity risk must be evaluated through the lens of patient safety. A standalone security risk register doesn't demonstrate that link.

How to fix it.

- Map each cybersecurity risk to a corresponding hazard and harm in the ISO 14971 file.



- Document how exploitability is translated into a probability of harm.
- Show the residual risk evaluation post-controls in both files consistently.

4. Secure Product Development Framework (SPDF) gaps

Category: SPDF / QMS

What reviewers see. Design controls don't show evidence of security activities at each phase: requirements, design, implementation, verification, and release.

Why it's flagged. Section 524B and FDA's Feb 3, 2026 final cybersecurity guidance expect a documented SPDF that integrates with the QMSR (21 CFR Part 820 / ISO 13485:2016). Missing artifacts at any phase signal an immature process.

How to fix it.

- Map every SPDF activity (requirements, threat modeling, secure coding, testing, vulnerability management) to a design control output.
- Provide objective evidence: review records, test results, training logs.
- Include a written SPDF policy that QMS auditors can trace.

Stuck on SBOM, threat modeling, or your SPDF? A 30-minute call with a senior expert can save weeks of rework. Talk to an expert.

5. Penetration testing scoped too narrowly or with the wrong methodology

Category: Penetration testing

What reviewers see. Pen test report covers only the web interface, uses automated scanning only, or was performed by a generalist firm without medical-device context.

Why it's flagged. FDA expects testing that exercises every interface (wireless, USB, BLE, cellular, cloud, service ports) using a methodology appropriate to a medical device's threat model.

How to fix it.

- Scope pen testing across all device interfaces and the supporting cloud/back-end ecosystem.
- Combine manual testing with automated tools; pure scans are insufficient.
- Engage testers with documented medical-device experience and provide them the threat model.

6. Missing coordinated vulnerability disclosure plan

Category: Post-market / CVD

What reviewers see. No published process for security researchers to report vulnerabilities, or no internal SLA for triage and remediation.

Why it's flagged. FDA explicitly calls out coordinated vulnerability disclosure (CVD) as a required element



of post-market cybersecurity. The absence of a documented program is a common deficiency.

How to fix it.

- Publish a CVD policy with a security contact, scope, and response SLAs.
- Define internal triage workflow tied to risk and patch release cadence.
- Reference ISO/IEC 29147 and ISO/IEC 30111 in your submission documentation.

7. Inadequate post-market cybersecurity monitoring plan

Category: Post-market surveillance

What reviewers see. Submission covers premarket controls but is silent on how vulnerabilities will be monitored, evaluated, and patched after clearance.

Why it's flagged. FDA evaluates premarket and post-market cybersecurity together. Without a credible monitoring and patch plan, the premarket controls don't stand on their own.

How to fix it.

- Document continuous monitoring sources (NVD, vendor advisories, CISA, ISAC feeds).
- Define risk-based remediation timelines and customer communication plans.
- Show how the SBOM is used operationally to detect new vulnerabilities.

8. Cybersecurity labeling deficiencies

Category: Labeling / documentation

What reviewers see. User-facing documentation is missing required cybersecurity transparency: SBOM access, end-of-support dates, network requirements, hardening guidance.

Why it's flagged. Cybersecurity labeling is now an explicit submission element per FDA's Feb 3, 2026 guidance. Reviewers check that users and IT departments have what they need to operate the device safely.

How to fix it.

- Include a dedicated cybersecurity section in IFU/labeling.
- Document supported configurations, ports, protocols, and end-of-support dates.
- Provide instructions for obtaining the SBOM and reporting vulnerabilities.

Want a second set of eyes before you submit? We do a fixed-fee gap analysis in days. Talk to an expert.

9. No documented SBOM lifecycle or maintenance plan

Category: SBOM / post-market

What reviewers see. An SBOM is provided, but there's no explanation of how it will be updated, validated,

and shared across the product's supported lifetime.

Why it's flagged. An SBOM that's accurate at submission but stale six months later doesn't satisfy FDA's intent. The lifecycle plan is just as important as the artifact itself.

How to fix it.

- Describe how the SBOM is regenerated on every build and every release.
- Document validation steps and the team accountable for accuracy.
- Define how customers can request the current SBOM post-market.

10. Architecture views missing required detail

Category: Security architecture

What reviewers see. Submission lacks global system view, multi-patient harm view, or updateability view, or doesn't show data flows and trust boundaries clearly.

Why it's flagged. FDA's Feb 3, 2026 final cybersecurity guidance (Appendix 2) is specific about the security architecture views required. Submissions that include only a single block diagram are routinely flagged.

How to fix it.

- Provide all required views: global system, multi-patient harm, updateability/patchability.
- Annotate trust boundaries, data classifications, and authentication points.
- Keep diagrams consistent with the threat model and design documentation.

11. Cryptographic controls not justified or documented

Category: Cryptography

What reviewers see. Algorithms, key sizes, and key management are mentioned but not justified against modern standards; deprecated algorithms still in use.

Why it's flagged. Reviewers expect a written cryptographic rationale: why each algorithm was chosen, where keys live, how they rotate, and how the design will age over the device's lifetime.

How to fix it.

- Document algorithms, key sizes, and protocols against NIST/FIPS guidance.
- Describe key generation, storage, rotation, and destruction.
- Plan for crypto-agility: how the device will move off deprecated algorithms in the field.

12. Update and patch mechanism not validated end-to-end

Category: Update / patch management



What reviewers see. The device can be updated, but there's no validated process showing authenticity, integrity, rollback, and failure handling for updates in the field.

Why it's flagged. Updateability is a required architecture view and a core post-market control. An unvalidated update path is one of the fastest ways to a deficiency letter.

How to fix it.

- Validate the update mechanism: signature verification, integrity checks, atomic install, rollback.
- Document the update workflow for users and clinical environments.
- Test the update path as part of system verification, including failure cases.

Pre-submission readiness checklist

If you can't check all twelve, you have known gaps that FDA is likely to flag. Use this as a go/no-go before you hit submit.

1. CycloneDX or SPDX SBOM with transitive dependencies and lifecycle plan. 2. Threat model with data flow diagrams, trust boundaries, and STRIDE/PASTA analysis. 3. Security Risk Assessment integrated with ISO 14971 risk file. 4. Documented SPDF with evidence at each design control phase. 5. Penetration test report covering all interfaces, performed with medical-device context. 6. Coordinated Vulnerability Disclosure (CVD) policy and intake process. 7. Post-market cybersecurity monitoring and patch plan. 8. Cybersecurity labeling: SBOM access, supported configs, end-of-support, hardening. 9. All required architecture views (global, multi-patient harm, updateability). 10. Cryptographic rationale with key management and crypto-agility. 11. Validated update mechanism with signature, integrity, and rollback testing. 12. Traceability matrix tying every cyber artifact to design controls and the QMS.

Timeline reality check

Teams routinely underestimate cyber effort. Here's what a complete cyber package typically takes for a moderate-complexity Class II connected device, when the work is done right the first time:

Artifact Typical effort --- --- SBOM tooling + lifecycle plan 2-3 weeks Threat model + data flow diagrams 3-5 weeks Security Risk Assessment integrated with ISO 14971 3-4 weeks SPDF documentation + traceability 3-6 weeks Penetration testing (all interfaces) 4-6 weeks Cybersecurity labeling + CVD program 2-3 weeks
--

Note: Some artifacts run in parallel. Most teams need 10-14 weeks of focused work; rework after an AI letter typically adds 8-12 additional weeks to clearance.

When to bring in a specialist partner

You don't need outside help for every submission. You probably do if any of these are true:

- This is your team's first 510(k), De Novo, or PMA with cybersecurity in scope.



- You've received an AI letter or RTA refusal citing cybersecurity.
- Your engineering team owns security alongside firmware and has limited bandwidth.
- Your launch date is fixed and a cyber deficiency would slip revenue.
- You need a defensible threat model and pen test from a firm FDA already recognizes.

| Want a senior expert to pressure-test your cyber package?

Book a free 30-minute strategy session. No sales rep, no obligation. We'll review where you are, flag the gaps FDA is most likely to hit, and give you a fixed-fee quote within 24-hours.

Explore our FDA premarket cybersecurity services, SBOM & lifecycle monitoring, threat modeling, penetration testing, and deficiency response programs.

Ready to talk through your roadmap?

[Book a Strategy Session →](#)

Source guide: 12-reasons-the-fda-rejects-medical-device-cybersecurity-submissions. For the most current version, visit bluegoatcyber.com/guides/12-reasons-the-fda-rejects-medical-device-cybersecurity-submissions.