BLUE GOAT CYBER
Medical Device Cybersecurity · FDA Specialists

FDA 2026 PREMARKET CYBERSECURITY DECODER

The 2026 FDA Cybersecurity Guidance Decoder

What changed in the Feb 3, 2026 final guidance, what reviewers now expect, and a 90-day path to a fully aligned premarket submission.

bluegoatcyber.com · 100% FDA submission success rate

WHY THIS MATTERS

The FDA's Feb 3, 2026 final premarket cybersecurity guidance.

On Feb 3, 2026 the FDA finalized its updated guidance, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*. It supersedes the Sept 27, 2023 version. Submissions filed after that date are reviewed against a higher, more specific bar - especially for SPDF evidence, SBOM machine-readability, and threat modeling rigor. This decoder distills what changed, what reviewers now expect, and the concrete artifacts your eSTAR needs to contain.

Key takeaway: If your last submission was before Feb 2026, your existing cybersecurity package is almost certainly out of date in at least three places. Plan a gap review before re-submitting.

1. What is a 'cyber device' under Section 524B?

Section 524B of the FD&C; Act (added by the Omnibus 2023 act) defines a cyber device as one that (a) includes software validated, installed, or authorized by the sponsor as a device or in a device, (b) has the ability to connect to the internet, and (c) contains technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats. The 2026 guidance reaffirms the FDA's broad reading of (b) - Bluetooth, cellular, USB tethered to a connected host, and offline devices that periodically sync all qualify.

2. The four pillars of a 2026-compliant submission

SPDF	Documented Secure Product Development Framework with *objective evidence* of execution - not just process descriptions. Reviewers want to see threat model outputs feeding design inputs, security risk assessments tied to ISO 14971, and verification records.
Threat Model	STRIDE-per-element (or equivalent) covering all data flows, trust boundaries, and external interfaces. Aligned to AAMI TIR57. Mitigations traced to design controls.
SBOM	Machine-readable in **SPDX 2.3+** or **CycloneDX 1.4+**. The 2026 guidance is explicit that PDFs and spreadsheets are not acceptable as the SBOM itself.
Security Testing	Manual, exploit-driven penetration testing by qualified humans against the actual interfaces - device hardware, companion apps, cloud APIs, wireless. Automated scans alone are insufficient.

3. What changed vs. the 2023 version

- **SBOM machine-readability is now mandatory.** 2023 'recommended', 2026 expects it. Include VEX statements to manage CVE noise.
- **SPDF evidence requirements are sharper.** Reviewers ask for traceability artifacts - threat model → security requirement → design control → V&V record - not just policy documents.
- **Postmarket plan must be in the premarket submission.** Vulnerability monitoring approach, coordinated disclosure policy, and patch cadence are reviewed up front.
- **Legacy / unsupported software is called out by name.** If your device ships with end-of-life OS components or libraries, you must justify with compensating controls.
- **AI/ML-enabled SaMD requires model-specific threats.** Data poisoning, model inversion, adversarial inputs, and prompt injection (for LLM features) belong in the threat model.

4. The eSTAR cybersecurity checklist

Drop these artifacts into the corresponding eSTAR sections:

- Cybersecurity Risk Assessment (linked to ISO 14971 risk file)
- Threat Model (STRIDE/PASTA, with diagrams and mitigation table)
- Architecture Views: global system, multi-patient harm view, updateability view, security use case view
- SBOM (CycloneDX 1.5 + VEX recommended)
- Vulnerability assessment of SBOM components (CVSS scored, with VEX status per CVE)
- Penetration test report (executive summary + technical detail + retest evidence)
- Security risk management report and traceability matrix
- Cybersecurity labeling for end users (security capabilities, hardening guidance)
- Postmarket cybersecurity management plan (monitoring, CVD, patching)

5. Common deficiency letter triggers (and how to avoid them)

PDF SBOM	Reviewer asks for machine-readable. Ship CycloneDX 1.5 from day one.
Generic threat model	If the model could apply to anyone's device, it will be rejected. Tie every element to *your* data flows and interfaces.
Pen test = scan output	Burp/Nessus output pasted into a Word doc reads as automated. Include manual exploitation chains, false-positive triage, and retest evidence.
Missing postmarket plan	Submissions without a credible monitoring + CVD + patching plan are routinely deficient. Include ownership, frequency, and reporting paths.

Unjustified residual risk	Every residual cybersecurity risk needs a benefit-risk rationale tied to the ISO 14971 file - not a hand-wave.

6. A 90-day path to a 2026-ready package

- **Days 1-15:** Architecture views, asset inventory, build the CycloneDX SBOM.
- **Days 15-35:** STRIDE-per-element threat model + security risk assessment integrated with ISO 14971.
- **Days 35-65:** Manual penetration testing across device, app, cloud, wireless. Remediate. Retest.
- **Days 65-80:** Postmarket plan, labeling, CVD policy, traceability matrix.
- **Days 80-90:** Internal review, eSTAR drop-in, mock review against the 2026 guidance checklist.

Key takeaway: Most teams that hit a deficiency letter under 2026 expectations do so because the SPDF evidence is thin or the SBOM is the wrong format. Both are fixable in days, not months - if you start from a 2026-aligned template.

READY FOR THE NEXT STEP?

Talk to a senior medical device security engineer.

We've contributed cybersecurity documentation, threat models, SBOMs, and pen test reports to **250+ FDA submissions** across 510(k), De Novo, and PMA pathways - with a **100% submission success rate**. If you're building a cyber device and want to go in with airtight artifacts on the first try, we should talk.

Book a Discovery Session
30 minutes. No slide deck. Bring your device profile and your top three questions.

bluegoatcyber.com/contact

WHAT WE DO

- **FDA premarket cybersecurity** - SPDF, threat model, SBOM, pen test, security risk assessment, eSTAR-ready package
- **FDA cybersecurity deficiency response** - rapid remediation when reviewers send a letter
- **Postmarket programs** - vulnerability monitoring, VEX, coordinated disclosure, patch validation
- **Legacy device remediation** - bring older devices up to current FDA expectations