

**BLUE GOAT CYBER**

Senior medical device cybersecurity

# THE MEDTECH SBOM COMPLIANCE PLAYBOOK

What the FDA actually expects for SBOMs, VEX, vulnerability monitoring, and postmarket cybersecurity under the Feb 3, 2026 final premarket guidance. Plain English, with templates you can use this week.

By the senior medical device security team at Blue Goat Cyber

## WHAT'S INSIDE

# Table of contents

|           |                                                           |       |
|-----------|-----------------------------------------------------------|-------|
| <b>01</b> | Why the FDA cares about SBOMs (and why your auditor will) | p. 3  |
| <b>02</b> | What the Feb 3, 2026 final guidance actually requires     | p. 4  |
| <b>03</b> | The five SBOM artifacts every premarket submission needs  | p. 5  |
| <b>04</b> | Building an SBOM that won't get flagged                   | p. 6  |
| <b>05</b> | Continuous vulnerability monitoring without the noise     | p. 7  |
| <b>06</b> | The postmarket evidence trail auditors look for           | p. 8  |
| <b>07</b> | Common pitfalls (and how to avoid them)                   | p. 9  |
| <b>08</b> | A 90-day SBOM compliance roadmap                          | p. 10 |
| <b>09</b> | About GoatWatch and next steps                            | p. 11 |

## SECTION 01 · REGULATORY CONTEXT

## Why the FDA cares about SBOMs

If you've sold a connected medical device in the last decade, your software stack has quietly become a regulatory artifact. The FDA no longer treats third-party components as someone else's problem. Under Section 524B of the FD&C Act (added by the Consolidated Appropriations Act, 2023), if you can't tell the agency exactly what's running inside your device and how you're monitoring it for vulnerabilities, your submission can be refused.

The Software Bill of Materials (SBOM) is the regulatory artifact that makes this possible: a structured inventory of every software component shipped with your device, open source, proprietary, and everything in between.

### WHY THIS MATTERS NOW

The FDA's **February 3, 2026 final premarket cybersecurity guidance** (which superseded the September 2023 guidance) is what the FDA enforces today. It defines the eSTAR v7.0 cybersecurity slot structure, the SBOM and VEX expectations, and the seven sections reviewers screen against before the 180-day clock starts.

### Three forces are converging

- **FDA enforcement.** Cybersecurity is a Refuse-to-Accept (RTA) criterion, not a recommendation, and the Feb 3, 2026 guidance gave reviewers a sharper checklist.
- **Health-system procurement.** Hospitals increasingly demand SBOMs and current MDS2 forms as a condition of purchase, often as RFP-gating items.
- **Threat reality.** Ripple20, Log4Shell, Curl CVE-2023-38545, and the 2024 XZ Utils backdoor each affected hundreds of medical device models. Manufacturers without SBOMs spent weeks just figuring out whether they were exposed.

## SECTION 02 · THE RULE ITSELF

## What the Feb 3, 2026 guidance requires

The FDA's guidance *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions* (final, February 3, 2026) is the authoritative document. It superseded the September 2023 final guidance and is what reviewers apply today. The rule applies to any device meeting the statutory definition of a "cyber device": software-containing, internet-capable, and presenting a cybersecurity risk. In practice, that is the vast majority of modern Class II and Class III submissions.

### Four concrete obligations under Section 524B

- **Submit a machine-readable SBOM** in CycloneDX 1.5+ or SPDX 2.3+, with NTIA minimum elements and a paired VEX document for any unresolved CVEs.
- **Demonstrate a vulnerability management process**, not just a policy. The Feb 3, 2026 guidance expects evidence the process actually runs (triage logs, SLAs, named owners).
- **Provide a coordinated vulnerability disclosure (CVD) plan** with a public security contact, consistent with ISO/IEC 29147 and 30111.
- **Plan for postmarket updates**, including a validated patch delivery mechanism and an updatability architecture view (eSTAR v7.0 Slot 4).

#### THE QUIET KILLER

Most submissions that fail RTA don't fail because the SBOM is missing, they fail because it's incomplete, in the wrong format, or contradicts other parts of the submission (the threat model in Slot 3 names a component the SBOM in Slot 5 doesn't). Format and cross-reference checks happen first; content depth is checked second.

## SECTION 03 · THE FIVE ARTIFACTS

## What every premarket submission needs

FDA reviewers look for five distinct artifacts. Missing any one of them is a common cause of Additional Information (AI) requests that delay clearance by 60 to 90 days. All five live in or feed eSTAR v7.0 cybersecurity slots.

| # | Artifact                     | Format / Slot                        | Common gap                                          |
|---|------------------------------|--------------------------------------|-----------------------------------------------------|
| 1 | Machine-readable SBOM        | CycloneDX 1.5+ / SPDX 2.3+ · Slot 5  | Hand-edited JSON; missing hashes or transitive deps |
| 2 | Component support status     | Table or appendix · Slot 5           | No EOL / EOS dates for OSS or COTS dependencies     |
| 3 | Known-vulnerability + VEX    | VEX (CycloneDX or CSAF) · Slot 5 / 6 | Stale CVE lookup; no VEX statements at submission   |
| 4 | Risk rationale per finding   | Narrative · Slot 6                   | Generic 'not exploitable' with no device context    |
| 5 | Update mechanism description | SPDF + architecture view · Slot 4    | No evidence patches actually reach fielded devices  |

**PRO TIP**

Generate VEX (Vulnerability Exploitability eXchange) statements alongside your SBOM, not after. The Feb 3, 2026 guidance treats VEX as the expected vehicle for documenting which CVEs are not exploitable in your device's deployment context. This saves weeks in postmarket triage and shortens AI-letter response time.

## SECTION 04 · BUILDING IT

## An SBOM that won't get flagged

A conforming SBOM is more than a dependency dump. The minimum data fields per NTIA's "Minimum Elements" framework are non-negotiable, but the difference between a passable SBOM and an excellent one is in the details.

### Required fields

- Supplier name
- Component name and version
- Unique identifier (PURL, CPE, or SWID)
- Dependency relationship (what depends on what)
- SBOM author
- Timestamp

### Fields that separate passing from professional

- Cryptographic hash of each component binary (SHA-256 minimum)
- License declaration with SPDX identifier
- Support status: actively maintained, EOL, or deprecated
- Source location for build reproducibility
- Known unknowns: components you couldn't fully resolve, documented as such

#### FORMAT CHOICE

If you're starting fresh, choose **CycloneDX 1.5+**. It has first-class support for VEX, hardware components (HBOM), and ML model bills of materials (MLBOM), all of which the FDA is signaling interest in. **SPDX 2.3+** is also fully accepted under the Feb 3, 2026 guidance and is fine if you already have tooling investment there.

## SECTION 05 · MONITORING

## Continuous monitoring without the noise

An SBOM submitted at clearance is a snapshot. By the time your device ships, half a dozen new CVEs likely affect components in it. By the time it has been in the field a year, that number is often in the hundreds.

The compliance question isn't "are there CVEs?" There always are. It's whether you have a defensible process for finding them, evaluating them, and acting on the ones that matter.

### What "defensible" looks like

- Automated daily ingestion from NVD, GitHub Security Advisories, vendor PSIRTs, and H-ISAC.
- Component-to-CVE matching using PURL or CPE, not package name string matching.
- Device-context triage: is the affected component reachable, on a network interface, and exercising the vulnerable code path?
- Exploitability scoring using EPSS and CISA KEV in addition to CVSS.
- Documented decision for every CVE: patch, mitigate, or accept (with rationale captured as a VEX statement).

#### THE NOISE PROBLEM

A typical infusion pump SBOM has 200 to 400 components. Without context-aware filtering, you'll triage 50 to 100 'new critical CVEs' per month, most of which don't affect your device. Teams that survive this build triage automation early and emit VEX statements as a byproduct.

## SECTION 06 · EVIDENCE

## The postmarket evidence trail auditors look for

In a postmarket inspection or AI request, the FDA doesn't want to hear that you have a process. The reviewers want to see it. The evidence trail should be reproducible from raw data with no manual reconstruction.

### The five evidence artifacts

- **Versioned SBOMs** for every released firmware or software build, retained for the device's supported life.
- **CVE triage log**: each finding, when it was detected, who reviewed it, and the disposition rationale.
- **VEX statements** documenting non-exploitable findings with technical justification (component reachability, configuration, threat model coverage).
- **Patch deployment records**: what shipped, to whom, and confirmation of installation.
- **Annual security review** summarizing posture, incidents, trend data, and KPI movement.

#### AUDIT-READY MEANS REPRODUCIBLE

If a reviewer asks "what did your SBOM look like for firmware v2.4.1 on March 12, 2026, and what CVEs were known then?", you should be able to answer in minutes, not weeks. Snapshot, don't reconstruct.

## SECTION 07 · PITFALLS

## Common mistakes (and how to avoid them)

---

### Treating the SBOM as a one-time deliverable

It's a living artifact. Generate it on every build, store it with the build, and diff it across releases.

### Only listing top-level dependencies

The FDA expects transitive dependencies too. A "shallow" SBOM is one of the fastest ways to fail RTA.

### Ignoring firmware and embedded OS components

Yes, that includes the BusyBox in your bootloader and the OpenSSL inside your TLS stack. Both have shipped with major CVEs.

### Submitting CVE lists from a single point in time, with no VEX

By the time the reviewer reads it, it is stale. Document your monitoring process and pair every unresolved CVE with a VEX statement.

### Outsourcing without auditing

If your contract manufacturer or SDK vendor provides components, you are still responsible for their SBOM data. Get it in writing as a supplier SLA.

### Confusing CVSS with risk

A 9.8 CVSS in a component you don't actually invoke is lower priority than a 5.4 in your authentication path. Document the difference using VEX and your threat model.

## SECTION 08 · ROADMAP

## A 90-day SBOM compliance roadmap

If you're starting from zero, 90 days is enough to reach defensible compliance for a single device line. Here's the sequence we use with clients.

| Phase       | Days    | Outcome                                                                                                                         |
|-------------|---------|---------------------------------------------------------------------------------------------------------------------------------|
| 1. Discover | 0 – 15  | Inventory build systems, identify all third-party components and firmware blobs, choose SBOM format (CycloneDX 1.5+ preferred). |
| 2. Generate | 15 – 35 | Integrate SBOM generation into CI/CD. Validate completeness against build artifacts. Produce first VEX baseline.                |
| 3. Monitor  | 35 – 60 | Stand up daily CVE ingestion against the SBOM. Define triage criteria, severity thresholds, and named owners.                   |
| 4. Evidence | 60 – 80 | Implement versioning and retention. Document the process in a Cybersecurity Management Plan (eSTAR v7.0 Slot 8).                |
| 5. Operate  | 80 – 90 | Run a tabletop exercise on a simulated CVE. Refine the playbook. You are now defensibly compliant.                              |

### WHERE TEAMS GET STUCK

Phases 1 and 3. Discovery always takes longer than expected because firmware components are scattered across vendor SDKs. Monitoring requires deciding how aggressive your triage thresholds are — too tight and you miss things, too loose and you drown.

## SECTION 09 · NEXT STEPS

## How GoatWatch fits in

GoatWatch by Blue Goat Cyber is the continuous SBOM risk management service built specifically for medical device manufacturers. We do exactly what Sections 5 and 6 of this playbook describe: automated ingestion, device-context triage, VEX-ready evidence — without the noise.

### What you get

- Daily CVE matching against your live SBOMs (CycloneDX and SPDX)
- Device-context impact triage that filters out non-exploitable findings
- VEX statements generated automatically with reviewer-ready rationale
- Versioned, audit-ready evidence retained for the device's supported life
- Senior MedTech security experts on call, not a ticket queue

#### READY TO TALK?

Book a free 30-minute discovery call with a senior medical-device security expert (not a sales rep). We'll walk through your current SBOM posture and identify the two or three changes that will most reduce your regulatory risk.

**[bluegoatcyber.com](https://bluegoatcyber.com) · (844) 939-4628**

*This guide is provided for educational purposes and does not constitute legal or regulatory advice. Always consult your regulatory affairs team and qualified counsel for submission-specific guidance.*