GUIDE

The Postmarket Cybersecurity Readiness Plan

Free Guide · Updated 2026 · FDA-Aligned The Postmarket Cybersecurity Readiness Plan Premarket → Launch → Operate What FDA expects, and when. A three-phase plan for the cybersecurity work that starts b

Free Guide · Updated 2026 · FDA-Aligned

Premarket → Launch → Operate

Phase 1 - Premarket Build

Before 510(k) filing

→

Phase 2 - Pre-Launch Activation

Before first ship

→

Phase 3 - Postmarket Operate

Part 1

The Executive Brief

FDA pushed cybersecurity left. It is no longer something you add after clearance - it is a documented, inspectable program FDA reviews as part of your 510(k), De Novo, or PMA. Miss it and your submission is refused. Operate it badly and your devices get recalled.

The one-paragraph version

Section 524B of the FD&C Act made cybersecurity a precondition for clearance: every “cyber device” submission must include a postmarket cybersecurity plan, SBOM, coordinated vulnerability disclosure (CVD) policy, and patch process. The FDA’s Feb 2026 final guidance and QMSR (21 CFR Part 820) incorporating IEC 81001-5-1 raised the bar further. Post-clearance, you now run an ongoing program: monthly CVE triage against your SBOM, quarterly KPI reporting, annual pen tests and IR exercises, and a MedWatch-reportable decision workflow when something goes wrong.

The timing nobody told you about

Before 510(k) Filing

Cybersecurity plan, SBOM baseline, CVD policy, patch process, and IR plan authored and reviewed as submission documents.

Before First Ship

All plans made operational: SBOM tooling live in CI/CD, vulnerability monitoring active, CVD inbox standing, MDS2 published.

Life of Device

Monthly triage, quarterly KPI reports, annual pen test and IR exercise, MedWatch decision support for every cybersecurity event.

What FDA can do at each phase

PhaseFDA Authority

Premarket (submission)Refuse to Accept (RTA) or issue AI letter

Post-clearance (inspection)483 observation, Warning Letter, consent decree

Post-clearance (incident)MedWatch report, recall, market withdrawal

Why this is uniquely hard for medical devices

Unlike enterprise software, medical devices have decade-long field lifespans, constrained update windows, patient-safety implications for every patch decision, and a regulatory framework that treats your postmarket security program as an inspectable quality record. A vulnerability that would be a one-hour hotfix in SaaS is a multi-month change-controlled event tied to 21 CFR Part 820 and ISO 14971.

Part 2

The Three Phases

Premarket Build · Pre-Launch Activation · Postmarket Operate. Each phase has specific deliverables, owners, and regulatory tie-ins. Use this section as your program roadmap.

Phase 1 - Premarket Build

Before 510(k) / De Novo / PMA filing

Author the complete postmarket program as submission documents. Every plan, policy, and process description FDA reviews on day one.

Premarket Build

Cybersecurity Risk Management Plan

Author the postmarket plan FDA reviews as part of your submission. Defines how you will identify, assess, and address cybersecurity vulnerabilities for the life of the device.

Deliverables

- Postmarket Cybersecurity Plan (governance, cadence, roles)
- Cybersecurity RACI across Product, Quality, Regulatory, Support
- Threat model + security architecture views (per AAMI TIR57)

Owners

Product Security Lead · VP Quality / Regulatory

FDA / Standards Tie

21 USC §524B(b)(1) and FDA guidance §V - the cybersecurity plan is a required element of a “cyber device” submission.

Premarket Build

SBOM Baseline

Generate the first complete Software Bill of Materials in a machine-readable format. This is the artifact FDA uses to evaluate your vulnerability monitoring capability.

Deliverables

- CycloneDX or SPDX SBOM from production build
- All transitive dependencies, version pins, suppliers
- SBOM maintenance and distribution policy

Owners

Engineering · Product Security

FDA / Standards Tie

FDA guidance §VI.B - machine-readable SBOM with transitive dependencies required. IEC 81001-5-1 §5.6 requires SBOM throughout lifecycle.

Premarket Build

Vulnerability Monitoring Plan

Document exactly how you will correlate SBOM components to CVE feeds after clearance, who triages, and what the SLAs are for each severity tier.

Deliverables

- Monitoring source list (NVD, CISA KEV, H-ISAC, vendor PSIRTs)
- Risk-based triage SLAs by CVSS severity
- Named triage owner and escalation path

Owners

Product Security · Quality

FDA / Standards Tie

FDA guidance §VI.A - monitoring must be documented and operational post-clearance. IEC 81001-5-1 §5.7 requires ongoing TPLC vulnerability tracking.

Premarket Build

Coordinated Vulnerability Disclosure (CVD) Policy

Publish the intake path and response process for external security researchers - a required submission element and a patient-safety expectation.

Deliverables

- CVD policy with security contact, scope, and response SLAs
- Internal triage workflow tied to patch cadence
- References to ISO/IEC 29147 and 30111

Owners

Product Security · Legal · Communications

FDA / Standards Tie

FDA guidance §VII - CVD is explicitly required. Absence of a documented program is a common deficiency.

Premarket Build

Patch & Update Process Description

Document the change-controlled workflow for delivering security patches: how updates are tested, signed, distributed, and validated in the field.

Deliverables

- Patch development and testing under 21 CFR 820 change control
- Update delivery mechanism (OTA, service, CDN)
- Rollback and failure handling procedures

Owners

Engineering · Regulatory · Quality

FDA / Standards Tie

FDA guidance §VI.C - updateability is a required architecture view. Update mechanism must be validated end-to-end.

Premarket Build

Incident Response Plan

Define the decision logic for cybersecurity incidents: triage, containment, MedWatch reporting threshold, customer notification, and corrective action.

Deliverables

- IR playbook with roles, comms tree, and escalation
- MedWatch reportability decision tree
- Corrective action and post-incident review process

Owners

Product Security · Regulatory Affairs · Executive Sponsor

FDA / Standards Tie

21 CFR 803 - cybersecurity events causing patient harm are MedWatch-reportable. FDA expects a documented decision process.

Need help building Phase 1 artifacts?

We author the full premarket cyber package - RTA-proof on §524B elements.

Our premarket services

Phase 2 - Pre-Launch Activation

Between clearance and first commercial unit

Make every premarket plan operational before Day 1. Plans on paper are not enough - the moment a device is in a hospital, the clock starts on CVD response, MDS2 currency, and MedWatch reporting.

Pre-Launch

Wire SBOM Tooling to CI/CD

SBOM generation runs automatically on every release build. Output is stored, queryable, and diffable. No manual steps.

Deliverables

- CycloneDX/SPDX SBOM generated on every build
- Per-device, per-version SBOM repository
- Supplier SBOM intake workflow operating

Owners

Engineering · DevSecOps

FDA / Standards Tie

FDA guidance + IEC 81001-5-1 §5.6 - SBOM is a living artifact maintained throughout the device lifecycle.

Pre-Launch

Activate Vulnerability Monitoring Feeds

Live correlation of SBOM components to NVD, CISA KEV, ICS-CERT, vendor PSIRTs, and H-ISAC. Daily digest routed to a named triage owner.

Deliverables

- SBOM ↔ CVE pipeline running in production
- Threat intel subscriptions active (H-ISAC, CISA, vendor PSIRTs)
- On-call rotation defined

Owners

Product Security · SOC / Managed Service Partner

FDA / Standards Tie

FDA guidance §VI.A - monitoring must be active, not aspirational, the moment devices are in the field.

Pre-Launch

Stand Up the CVD Inbox

security@ inbox monitored, security.txt published on company and product domains, PGP key distributed, acknowledgement workflow live.

Deliverables

- security.txt live at /.well-known/security.txt
- security@ inbox routed to 24/7 monitored channel
- Acknowledgement SLA ≤ 72h verified by test report

Owners

Product Security · IT · Communications

FDA / Standards Tie

FDA guidance §VII - CVD must be operational, with a published intake path, before devices ship.

Pre-Launch

Publish MDS2 + Customer Security Pack

Hospitals, IDNs, and procurement teams expect a current MDS2 and a security documentation pack at point of sale. Missing either is now an RFP gating issue.

Deliverables

- MDS2 (HIMSS / NEMA) per device model
- Customer-facing security white paper
- SBOM customer-distribution policy (NDA-gated)

Owners

Product Marketing · Product Security · Customer Success

FDA / Standards Tie

FDA guidance §VI.D + IMDRF transparency principles - timely customer communication is part of a recognized program.

Pre-Launch

Tabletop the IR Plan

Run at least one full tabletop cybersecurity incident exercise. Validate communications tree, MedWatch decision logic, and corrective-action workflow before any real event.

Deliverables

- Tabletop exercise after-action report
- Updated IR plan with gaps addressed
- MedWatch decision tree signed off by Regulatory Affairs

Owners

Product Security · Regulatory Affairs · Quality

FDA / Standards Tie

FDA guidance - IR readiness is part of the inspectable postmarket program. Tabletop evidence satisfies both FDA and notified bodies.

Pre-Launch

Train QMS, Lock Vendor SLAs

Every quality and engineering team member understands their role in the cyber program. Every third-party software vendor has a contractual obligation to provide CVE notifications and SBOMs.

Deliverables

- Cybersecurity training records in QMS
- Vendor security SLA template executed with key suppliers
- Cyber program integrated into 21 CFR 820 change control SOPs

Owners

Phase 3 - Postmarket Operate

Life of device - ongoing

Run the continuous loop: monthly triage, quarterly KPI review, annual exercises, and event-driven response. Every cycle produces inspectable evidence for FDA, notified bodies, and your board.

Monthly

CVE Triage + SBOM Refresh

Every new CVE is correlated against the device SBOM. Each match is triaged to closure - patch, risk acceptance, or compensating control - within the defined SLA.

Deliverables

- Monthly triage report (open, resolved, accepted risk)
- Updated SBOM reflecting any component changes
- Triage records in QMS

Owners

Product Security · Quality

FDA / Standards Tie

IEC 81001-5-1 §5.7 + FDA guidance §VI.A - ongoing monitoring with documented disposition is the core of an inspectable postmarket program.

Monthly

Patch Delivery Under Change Control

Security patches are developed, tested, approved, and delivered through the 21 CFR 820 change control process. No out-of-band hotfixes without a documented rationale.

Deliverables

- Change record for every security patch
- Regression test evidence
- Customer patch notification and deployment guide

Owners

Engineering · Regulatory Affairs · Quality

FDA / Standards Tie

QMSR (21 CFR Part 820) - patches are device changes and require design history file documentation.

Quarterly

KPI Review + MDS2 Currency

Measure the eight postmarket cybersecurity KPIs, review against thresholds, and escalate if any metric is out of bounds. Update MDS2 for any product change.

Deliverables

- Quarterly KPI dashboard (8 metrics, see Part 3)
- Updated MDS2 if product configuration changed
- Board / exec summary if any KPI breaches threshold

Owners

Product Security · Quality · VP Regulatory

FDA / Standards Tie

FDA guidance §VI.D - transparency and communication cadence with customers is part of the recognized program.

Annually

Pen Test, IR Exercise, Board Report

Annual penetration test across all device interfaces, full-scale incident response exercise, and an executive board report on the state of the cybersecurity program.

Deliverables

- Annual pen test report with remediation tracking
- IR exercise after-action report
- Board cybersecurity briefing deck

Owners

Product Security · Executive Sponsor · Board

FDA / Standards Tie

FDA guidance - annual pen testing and IR exercises are part of a credible, demonstrable postmarket program.

Event-Driven

MedWatch, Recall, EOL

When a cybersecurity event occurs - a vulnerability causing patient harm risk, a confirmed exploit, or an end-of-life component with no patch - follow the defined escalation and reporting workflow.

Deliverables

- MedWatch reportability decision and filing
- Recall or field safety corrective action if required
- EOL component migration plan activated

Owners

Regulatory Affairs · Executive Sponsor · Legal

FDA / Standards Tie

21 CFR 803 + FDA postmarket guidance - cybersecurity events with patient harm risk are MDR-reportable. FDA expects a documented and practiced decision process.

Always-On

Inspectable Evidence Package

Every cycle produces records that can be pulled for an FDA inspection, notified body audit, or customer due diligence request with no scramble.

Deliverables

- Triage logs, patch records, training records in QMS
- Current SBOM, CVD log, and KPI history
- Audit-ready evidence package per device per year

Owners

Quality · Product Security

FDA / Standards Tie

QMSR (21 CFR Part 820) - cybersecurity records are quality records. FDA inspectors expect to pull them on-site.

Part 3

The KPI Dashboard

Eight metrics every postmarket cybersecurity program reports on. If any metric is out of bounds, it goes to the board.

MetricDefinitionTargetOwner

Mean Time to Triage (MTTT)Days from CVE publication to disposition decision≤ 5 days for Critical/ HighProduct Security

Mean Time to Patch (MTTP)Days from triage to patch availability≤ 30d Critical, ≤ 90d HighEngineering

SBOM Coverage% of shipping components with version-pinned SBOM entry100%Engineering

CVD Response Rate% of external reports acknowledged within SLA100% within 72hProduct Security

Open Critical/High VulnerabilitiesCount of unresolved Critical or High CVEs past SLA0 overdueProduct Security · Quality

MDS2 CurrencyAge of current MDS2 vs. last product change≤ 90 days staleProduct Marketing

IR Exercise CadenceMonths since last tabletop exercise≤ 12 monthsProduct Security · RA

Pen Test CurrencyMonths since last full-scope pen test≤ 12 monthsProduct Security

Part 4

How Blue Goat Cyber Fits

You do not need to hire a security team to run this plan. Blue Goat Cyber is the MedTech-only cybersecurity firm that builds the premarket package with you, activates the program before launch, and operates the postmarket loop on a fixed-fee subscription.

Phase 2 - Activate

We wire SBOM tooling, monitor CVE feeds, stand up your CVD inbox, publish your MDS2, and run your first IR tabletop - before the first device ships.

Phase 3 - Operate

Monthly triage, quarterly KPI report, annual pen test, MedWatch decision support, and an inspectable evidence package - on a fixed-fee retainer.

Why MedTech leaders choose us

- Every engagement is a medical device. We don't split focus with enterprise IT clients.
- The team that authored your §524B plan is the team that operates it after clearance - no handoff, no ramp-up.
- 250+ submissions cleared with zero rejections. We carry the FDA clearance guarantee.
- Post-market services on a fixed-fee subscription - predictable cost, no scope creep.
- When an incident happens, we are already on call with your device context loaded.

Ready to talk through your roadmap?

Book a Strategy Session →

Source guide: postmarket-cybersecurity-readiness-plan. For the most current version, visit bluegoatcyber.com/guides/postmarket-cybersecurity-readiness-plan.