BLUE GOAT CYBER
Medical Device Cybersecurity

MEDICAL DEVICE CYBERSECURITY GUIDE

Secure Product Development Framework (SPDF): FDA Playbook

The secure product development framework (SPDF) for medical devices: what FDA guidance recommends, how it maps to IEC 81001-5-1, the eight pillars, and a checklist.

Reviewed 2026-10-22

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

IN BRIEF

A Secure Product Development Framework is a lifecycle approach to reducing cybersecurity vulnerabilities. Section IV.A.1 of the FDA's February 3, 2026 final guidance encourages its use but permits other approaches that satisfy the QMSR. Section 524B establishes separate obligations for covered cyber-device submissions, not a requirement to use the SPDF name. This playbook's eight pillars are Blue Goat Cyber's practical organization of activities, not an FDA-mandated eight-part framework.

A practical, ungated guide to building a Secure Product Development Framework (SPDF) for FDA review - the eight pillars, the artifacts each one produces, and a pre-submission readiness checklist you can score yourself against.

SPDF PLAYBOOK · FDA CYBERSECURITY GUIDE

A practical, ungated guide to building a Secure Product Development Framework for FDA review. The eight pillars, the artifacts each one produces, and a pre-submission readiness checklist you can score yourself against this week.

8 pillars covered · 15-point checklist · effort timeline included

275+ FDA submissions supported, zero cybersecurity rejections · **8** SPDF pillars · device-specific evidence planning

Why the SPDF is Now the Center of FDA Cybersecurity Review

Section 524B of the FD&C Act gives the FDA the explicit authority to refuse any premarket submission for a cyber device that doesn't meet cybersecurity requirements. the FDA's February 2026 premarket cybersecurity guidance, AAMI SW96, and IEC 81001-5-1 support secure lifecycle activities integrated with your QMS. Section IV.A.1 encourages an SPDF but expressly allows other approaches that meet the QMSR. The eight pillars below are our planning structure, not mandatory FDA categories.

Blue Goat track record: 275+ FDA submissions supported, zero cybersecurity rejections. We see the same pattern: teams that pass review do not have eight separate security documents. They have **one SPDF, with eight pillars feeding consistent artifacts** into the design history file. This playbook is how we build it. If you want senior help setting it up, see our medical device cybersecurity consulting service.

How to Use This Playbook

1. Read each pillar as a **self-assessment**: do you have the artifact, and is it at the depth FDA guidance recommends?
2. Use the **checklist at the end** to score your submission readiness across all 15 go/no-go criteria.
3. Where you find a gap, the artifact list is **concrete enough to start work on Monday**.

The Eight Pillars of an SPDF for FDA Submissions

Each pillar includes a definition, why FDA cares, and the concrete artifacts you need to build a defensible submission package.

SPDF Governance & QMS Integration

What it is. A written Secure Product Development Framework policy that lives inside your ISO 13485 QMS and references IEC 62304 software lifecycle activities. It defines roles, escalation paths, and the security gates that block a release.

Why FDA cares. the FDA's February 2026 premarket cybersecurity guidance encourages an SPDF as a lifecycle process rather than a single document. Section 524B(b)(2) separately requires processes providing reasonable assurance of cybersecurity for covered cyber devices; it does not prescribe an SPDF. Reviewers look for evidence that security decisions are made by accountable owners and traced through your QMS like every other design control.

Artifacts you need.

- **SPDF policy document** mapped to QMS procedures
- **RACI matrix** covering security architect, QA, regulatory, and engineering
- **Definition of Done** for each design phase including security exit criteria

Security Requirements & Design Inputs

What it is. Cybersecurity requirements derived from intended use, risk, and applicable standards (FDA 524B, AAMI SW96, IEC 81001-5-1, IEC 62443-4-2). Each requirement is testable and traced to a design output.

Why FDA cares. Without explicit security requirements, there is nothing to verify against. Reviewers commonly flag submissions where security controls appear in implementation but never in requirements, breaking traceability.

Artifacts you need.

- **Security requirements specification** with unique IDs and rationale
- **Traceability** from each requirement to threats, controls, tests, and design outputs
- **Mapping to applicable standards** and regulatory clauses

Threat Modeling & Architecture Views

What it is. Data flow diagrams with trust boundaries, a STRIDE or PASTA threat enumeration, and the four architecture views FDA guidance recommends: global system, multi-patient harm, updateability, and security use case views.

Why FDA cares. the FDA's February 2026 guidance is specific about the views required. Submissions with a single block diagram and a generic STRIDE table are routinely held with deficiencies tied to threat model depth and architecture clarity.

Artifacts you need.

- **Data flow diagrams** covering every interface, trust boundary, and external entity
- **Threat register** linking each threat to a control, test, or accepted residual risk
- **All four architecture views**, kept consistent with the threat model

Stuck on threat modeling, architecture views, or risk integration? A 30-minute call with a senior expert can save weeks of rework. Talk to an SPDF expert →

Security Risk Management Integrated with ISO 14971

What it is. A Security Risk Assessment that scores exploitability in place of probability, pairs it with the ISO 14971 severity of harm (see how the two matrices share exploitability), and lives inside the same risk file as your ISO 14971 hazard analysis, not in a parallel spreadsheet.

Why FDA cares. Section 524B and the premarket guidance are explicit: cybersecurity risk must be evaluated through patient safety. A standalone security risk register without 14971 linkage is one of the most common deficiency triggers.

Artifacts you need.

- **Security Risk Assessment** with exploitability-to-harm mapping
- **Bidirectional traceability** between security risks and 14971 hazards
- **Residual risk evaluation** reflected consistently in both files

Is Your SPDF Ready for FDA Review?

Blue Goat track record: 275+ FDA submissions supported, zero cybersecurity rejections. Let us review your SPDF gaps before you submit.

Book a Free 30-Minute Strategy Session →

Secure Implementation, SBOM, & SOUP

What it is. Secure coding standards, code review with security checklists, dependency hygiene, and a CycloneDX or SPDX Software Bill of Materials regenerated on every build with a documented lifecycle plan.

Why FDA cares. Section 524B requires an SBOM, and FDA guidance recommends a machine-readable SBOM that supports continuous vulnerability monitoring, plus evidence that third-party and SOUP components are evaluated, not just inventoried.

Artifacts you need.

- **Secure coding standard** tied to language and toolchain in use
- **CycloneDX or SPDX SBOM** with transitive dependencies, suppliers, versions, and licenses
- **SOUP analysis** with vulnerability assessment and rationale for use

Verification: Static Analysis, Fuzzing, & Penetration Testing

What it is. A layered test program: SAST and SCA in CI, protocol fuzzing on critical interfaces, and end-to-end penetration testing across every interface (wired, wireless, BLE, cellular, USB, cloud, service ports).

Why FDA cares. FDA guidance recommends testing scoped to the threat model and performed with medical-device context. Pure automated scans, web-only pen tests, and reports from generalist firms without medical experience are routinely flagged.

Artifacts you need.

- **SAST/SCA configuration and results** integrated into the design history file
- **Penetration test report** scoped across all interfaces, written for FDA audience
- **Fuzz testing results** on protocols handling untrusted input

Want a second set of eyes on your SPDF before you submit? We scope a fixed-fee gap analysis around your existing evidence. Talk to an SPDF expert →

Cybersecurity Labeling & Coordinated Vulnerability Disclosure

What it is. User-facing cybersecurity transparency: a labeling section covering supported configurations, network requirements, end-of-support dates, SBOM access, and a published Coordinated Vulnerability Disclosure (CVD) program with intake and SLAs.

Why FDA cares. Cybersecurity labeling and CVD are explicit submission elements. Reviewers verify that customers, IT departments, and security researchers have what they need to operate the device and report issues.

Artifacts you need.

- **Cybersecurity section in IFU/labeling** with hardening guidance and EOS dates
- **Published CVD policy** referencing ISO/IEC 29147 and 30111
- **Internal triage workflow** with risk-based response SLAs

Post-Market Monitoring, Patching, & TPLC

What it is. A Total Product Lifecycle (TPLC) plan that operationalizes the SBOM: continuous monitoring of vulnerabilities via NVD and CISA KEV, risk-based patch timelines, validated update mechanisms, and customer communication.

Why FDA cares. FDA evaluates premarket and post-market cybersecurity together. A strong premarket package with no credible monitoring or patch plan does not stand on its own.

Artifacts you need.

- **Vulnerability monitoring sources** and triage workflow tied to the SBOM
- **Validated update mechanism**: signature, integrity, atomic install, rollback
- **Customer communication and patch deployment plan** with SLAs

Pre-Submission SPDF Readiness Checklist

Use these fifteen items as an internal planning checklist, not a mandatory FDA pass/fail screen. Document applicability and alternative evidence for your device.

1. Documented secure development approach, whether an SPDF or another approach satisfying the QMSR, integrated with the QMS and IEC 62304 lifecycle
2. Security requirements specification with traceability to threats, controls, and tests
3. Threat model with data flow diagrams and STRIDE/PASTA analysis
4. All four FDA architecture views (global, multi-patient harm, updateability, security use case)
5. Security Risk Assessment integrated with the ISO 14971 risk file
6. CycloneDX or SPDX SBOM with transitive dependencies and lifecycle plan
7. SOUP analysis with vulnerability assessment for each component
8. SAST/SCA in CI with results in the design history file
9. Penetration test covering all interfaces, performed with medical-device context
10. Fuzz testing on protocols handling untrusted input
11. Cybersecurity labeling with hardening guidance, EOS dates, and SBOM access
12. Coordinated Vulnerability Disclosure policy with published intake and SLAs
13. Validated update mechanism with signature, integrity, and rollback testing
14. Post-market monitoring plan with risk-based patch timelines
15. Separate Section 524B obligations (postmarket vulnerability plan, cybersecurity and update processes, and SBOM) from guidance-recommended risk management, labeling, and traceability evidence

SPDF Effort, Calibrated

Build the schedule from your current evidence, device complexity, engineering availability, test access, and remediation needs. Several workstreams can run in parallel, but testing and manufacturer approvals create dependencies.

Workstream	Inputs and dependencies
Governance and requirements	QMS procedures, assigned owners, and intended use
Threat model and architecture	Current design, interfaces, and trust boundaries
Security risk management	Exploitability rationale, safety linkage, and manufacturer decisions
SBOM and component assessment	Build inventory, suppliers, versions, and vulnerability evidence

Workstream	Inputs and dependencies
Security testing	Stable device, threat-based scope, and remediation access
Labeling and postmarket planning	Supported lifetime, disclosure workflow, and update process

Agree device-specific milestones after the gap review. Neither a first SPDF nor an AI response has a universal completion time.

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:

- **First 510(k), De Novo, or PMA**, This is your team’s first submission with cybersecurity in scope.
- **AI Letter or RTA Refusal**, You’ve received a deficiency response citing cybersecurity or SPDF gaps.
- **Limited Bandwidth**, Your engineering team owns security alongside firmware and has limited bandwidth.
- **Fixed Launch Date**, Your launch date is fixed and a cyber deficiency would slip revenue.
- **Defensible Threat Model Needed**, You need a defensible threat model and pen test from practitioners with relevant medical-device cybersecurity experience.

How Blue Goat Cyber approaches SPDF work

Every FDA package we ship starts with an SPDF gap assessment against the eight pillars above. We do not sell a framework deck. We deliver the artifacts the reviewer opens: the threat model, the security risk assessment, the SBOM, the design and architecture views, the pen test report, the CVD and patch policies, the postmarket monitoring plan, and the labeling section. Each artifact maps to an applicable statutory obligation or a recommendation in the February 3, 2026 final premarket cybersecurity guidance. Our eight-pillar assessment does not make the SPDF itself mandatory.

Our senior team (CISSP, OSCP, and former military red-teamers) authors the package with your engineering and regulatory leads, then defends it through submission. If the FDA raises a cybersecurity question, we answer it at no extra cost until the cybersecurity portion is closed. Track record: 275+ FDA submissions supported, zero cybersecurity rejections.

For teams already mid-submission, we scope a pressure-test on your existing SPDF and hand back a prioritized fix list before you send.

Frequently asked questions

What is the SPDF and does the FDA require it?

No. Section IV.A.1 of the FDA's February 3, 2026 final guidance encourages an SPDF but permits other approaches that meet the QMSR. Manufacturers must satisfy applicable quality-system requirements and, for covered cyber devices, the separate Section 524B obligations. An SPDF is one way to organize lifecycle activities and evidence, not a mandatory named framework or standalone submission document.

Do the eight SPDF pillars map to a specific standard?

Yes. The pillars align with AAMI TIR57, ANSI/AAMI SW96:2023, IEC 81001-5-1, and the process expectations in ISO 14971 and IEC 62304. The February 2026 guidance references these standards as the operational interpretation of Section 524B. When we build an SPDF package we map each pillar to the specific clause of the standard so the reviewer can trace requirement, evidence, and residual risk in one path.

How long does it take to stand up an SPDF from scratch?

The schedule depends on existing QMS procedures, design evidence, engineering availability, test access, and remediation. Start with a gap assessment and agree milestones for the device and submission pathway instead of relying on a generic duration.

Can we reuse SPDF artifacts across multiple 510(k) submissions?

Yes, if they were built to be modular. The threat model, SBOM tooling, CVD policy, and postmarket monitoring plan are typically reusable across a product family. Device-specific artifacts (architecture views, pen test report, security risk assessment) have to be regenerated per submission. Teams that structure the SPDF as a shared QMS asset save weeks per subsequent clearance.

What is the difference between SPDF and SSDLC?

SSDLC is a general software security lifecycle used across industries. The SPDF is the medical-device-specific expression of that lifecycle, extended to cover premarket submission evidence, postmarket vulnerability management, and coordinated disclosure. Every SPDF is an SSDLC, but not every SSDLC meets FDA expectations. The 2026 guidance recommends SPDF-specific artifacts that a generic SSDLC will not produce.

What happens if the FDA cites SPDF gaps in a deficiency letter?

You get a hold on your submission until you respond. The most common response requires (a) revised SPDF documentation showing the pillar the reviewer cited is now covered, (b) evidence that the process is embedded in your QMS, not a one-off, and (c) an updated postmarket monitoring plan that closes the loop. Ignoring the deficiency or responding without process evidence usually triggers a second deficiency letter.

Want a Senior Expert to Pressure-Test Your SPDF?

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

275+ FDA submissions supported, zero cybersecurity rejections · **8** SPDF pillars

Book Strategy Session → (844) 939-4628

Related SPDF reading

- CI/CD Security Gates for Medical Devices: SPDF in Practice
- SPDF Cybersecurity Documentation: FDA Guidance Recommendations
- SPDF and IEC 62304 Mapping for Medical Device Cybersecurity
- SPDF vs SSDLC: What Medtech Teams Get Wrong
- SPDF vs TPLC in Medical Device Cybersecurity

Free tools for this

- SPDF Gap Checker - find the gaps between your development process and the SPDF that FDA guidance describes.

Current web guide: bluegoatcyber.com/guides/medical-device-cybersecurity-spdf-playbook

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.