



GUIDE

The SPDF Playbook for FDA-Ready Medical Devices

SPDF PLAYBOOK · FDA CYBERSECURITY GUIDE The SPDF Playbook for FDA-Ready Medical Devices
A practical, ungated guide to building a Secure Product Development Framework that FDA accepts.
The eight pillar

SPDF PLAYBOOK · FDA CYBERSECURITY GUIDE

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

Overview

- 250+ - Submissions
- Zero - Rejections
- 8 - SPDF Pillars
- +8-12w - AI Letter Delay (WHY IT MATTERS)

Why the SPDF is Now the Center of FDA Cybersecurity Review

Section 524B of the FD&C Act gives FDA the explicit authority to refuse any premarket submission for a cyber device that doesn't meet cybersecurity requirements. FDA's February 2026 premarket cybersecurity guidance, AAMI SW96, and IEC 81001-5-1 all converge on the same expectation: a documented, repeatable Secure Product Development Framework integrated with your QMS.

After 250+ FDA submissions with 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.

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 expects? 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 FDA-Ready SPDF

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

WHY FDA CARES

FDA's February 2026 premarket cybersecurity guidance and Section 524B treat the SPDF as a process artifact, not a single document. 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

PILLAR 2 · REQUIREMENTS

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

PILLAR 3 · THREAT MODELING

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 expects: global system, multi-patient harm, updateability, and security use case views.



WHY FDA CARES

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

PILLAR 4 · RISK MANAGEMENT

Security Risk Management Integrated with ISO 14971

WHAT IT IS

A Security Risk Assessment that translates exploitability into probability of harm 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

FREE STRATEGY SESSION

Is Your SPDF Ready for FDA Review?

Our experts have guided 250+ FDA submissions without a single cybersecurity rejection. Let us review your SPDF gaps before you submit.

Book a Free 30-Minute Strategy Session →

PILLAR 5 · IMPLEMENTATION

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

FDA expects 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

PILLAR 6 · VERIFICATION

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

Reviewers expect 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 do a fixed-fee gap analysis in days. Talk to an SPDF expert →

PILLAR 7 · LABELING & CVD

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

PILLAR 8 · POST-MARKET

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

If you cannot check all fifteen, you have known gaps that FDA is likely to flag.

1. Written SPDF policy 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
 - CycloneDX or SPDX SBOM with transitive dependencies and lifecycle plan
7. SOUP analysis with vulnerability assessment for each component
 - SAST/SCA in CI with results in the design history file
 - 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

- Section 524B documentation set: Risk Management Report, Management Plan, Labeling, Traceability

| SPDF Effort, Calibrated

For a moderate-complexity Class II connected device, this is what a complete SPDF build typically looks like when the work is done right the first time. Several pillars run in parallel.

SPDF PILLAR

TYPICAL EFFORT

SPDF policy + QMS integration

1-2 weeks

Security requirements + traceability

2-3 weeks

Threat model + architecture views

3-5 weeks

Security risk + 14971 integration

3-4 weeks

SBOM tooling + SOUP analysis

2-3 weeks

SAST/SCA + penetration testing

4-6 weeks

Labeling + CVD program

2-3 weeks

Post-market plan + update validation

2-3 weeks

▲ Timeline Reality: Most teams need 10-14 weeks of focused work for a first SPDF. Rework after an FDA AI letter typically adds 8-12 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:

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 a firm FDA already recognizes.

| 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 FDA is most likely to hit, and give you a fixed-fee quote within 24 hours.

- 250+ - Submissions
- Zero - Rejections
- 8 - SPDF Pillars

Ready to talk through your roadmap?

[Book a Strategy Session →](#)

Source guide: [medical-device-cybersecurity-spdf-playbook](#). For the most current version, visit [bluegoatcyber.com/guides/medical-device-cybersecurity-spdf-playbook](#).