BLUE GOAT CYBER
Medical Device Cybersecurity · FDA Specialists

POSTMARKET VDP / CVD PROGRAM BLUEPRINT

Postmarket Vulnerability Disclosure & CVD Blueprint

An FDA-aligned Coordinated Vulnerability Disclosure program: policy, intake, triage SLAs, advisories, and reviewer-ready evidence.

bluegoatcyber.com · 100% FDA submission success rate

WHY THIS MATTERS

Stand up an FDA-aligned CVD program in 60 days.

The FDA's 2026 final premarket cybersecurity guidance requires a credible **postmarket cybersecurity plan** in the submission itself - including a Coordinated Vulnerability Disclosure (CVD) policy, monitoring approach, and patch cadence. Section 524B(b)(1) of the FD&C Act makes a 'plan to monitor, identify, and address postmarket cybersecurity vulnerabilities' a statutory submission requirement. This blueprint gives you the policy, the operating model, and the evidence reviewers and researchers expect.

Key takeaway: A CVD program is not a security.txt file. Reviewers, researchers, and hospital customers all want to see a policy, a working intake, real triage SLAs, and a track record of advisories - not just an email address.

1. The standards your program must align to

ISO/IEC 29147:2018	Vulnerability disclosure - the external-facing process. Defines policy, intake, coordination, and publication expectations.
ISO/IEC 30111:2019	Vulnerability handling - the internal process. Receipt, verification, resolution, post-resolution review.
FDA 2026 guidance	Postmarket plan content for premarket submissions - monitoring, CVD, patching, communications.
Section 524B(b)(1)	Statutory requirement for a postmarket vulnerability monitoring & disclosure plan.
CISA CVD process	Coordination path for ICS-MEDICAL advisories when impact is broad or upstream.

2. The eight pillars of a working CVD program

- **Public VDP policy page** - scope, safe harbor, channels, SLA commitments.
- **Multiple intake channels** - web form, security@ alias, PGP key, optional bug-bounty platform.
- **Internal triage workflow** tied to your QMS / CAPA system - every report is a tracked record.
- **CVSS + clinical-impact scoring rubric** - mapped to ISO 14971 risk levels.
- **Patch / mitigation development** with V&V evidence and regression testing.
- **Customer advisory + MDS^2 update + CISA coordination** for broad-impact issues.
- **Public CVE assignment** via CNA (apply directly or coordinate via MITRE root).

- **KPIs and continuous improvement loop** - measure, review, improve.

3. VDP policy template - required sections

Scope	List in-scope products + versions and out-of-scope items (third-party SaaS, retired models). Be specific - vague scope deters good-faith research.
Safe harbor	Commit not to pursue legal action against researchers who follow the policy. Reference DOJ CFAA guidance + DMCA Section 1201 research exemption.
Channels	Web form, security@yourcompany.com, PGP fingerprint, optional bug-bounty platform link.
Researcher expectations	No patient harm, no service disruption, no PHI exfiltration, give 90 days before public disclosure.
Our commitments	Acknowledge in 3 business days; triage in 10; status updates every 14 days; credit researchers (with consent).
Exclusions	Out-of-scope vulnerability classes (theoretical DoS without exploit, missing best-practice headers without impact).

4. Triage SLAs reviewers expect

Acknowledge	Within 3 business days of receipt - even if just an auto-reply with a tracking ID.
Initial triage + reproduction	Within 10 business days. Confirm scope, severity, and reproducibility.
Critical (CVSS 9.0+ or patient safety)	Mitigation guidance to customers in 30 days; patch in 60. CISA coordination engaged.
High (CVSS 7.0-8.9)	Patch in 90 days. Customer advisory at release.
Medium / Low	Bundle into next scheduled release. Public disclosure within 180 days.

5. The intake -> triage -> advisory workflow

- **Intake** - report received via channel, auto-acknowledged with ticket ID, logged in tracking system.
- **Triage** - security engineer reproduces, scopes, scores (CVSS + clinical impact), opens CAPA if confirmed.
- **Risk assessment** - update threat model and ISO 14971 risk file. Decide: patch, mitigate, or accept.
- **Development** - patch built, regression-tested, V&V'd against the security requirement that failed.
- **Coordination** - notify CISA for broad-impact issues. Coordinate disclosure timeline with researcher.
- **Disclosure** - publish customer advisory, update MDS^2, request CVE, post to your security advisories page.
- **Postmortem** - root-cause review feeds back into SPDF, threat model, and SDLC.

6. CVSS + clinical-impact scoring rubric

Critical	CVSS 9.0+ *or* direct patient-safety impact (unauthorized therapy, sensor falsification, life-support DoS).
High	CVSS 7.0-8.9 with realistic exploit path; PHI exfiltration at scale; broad fleet compromise.
Medium	CVSS 4.0-6.9; limited blast radius; requires authenticated attacker or local access.
Low	CVSS < 4.0; informational; defense-in-depth improvements.

7. Customer advisory + CISA coordination

When a confirmed vulnerability affects fielded devices, you owe customers a clear, actionable advisory. For broad-impact issues, coordinate with CISA so the same information appears in an ICS-MEDICAL advisory -

hospitals trust that channel.

Customer advisory minimum content

- Affected products and software versions
- CVE identifier(s) and CVSS score
- Vulnerability description (technical + clinical impact in plain language)
- Mitigations available today (configuration, network controls)
- Patch availability and update procedure
- Acknowledgement of the reporting researcher (with consent)
- Contact for follow-up questions

8. Reviewer-ready evidence pack

- Public VDP policy URL + PDF snapshot in the submission
- Process diagrams (intake -> triage -> advisory)
- Sample anonymized triage records (showing SLAs were met)
- Two or three published advisories (or template if pre-launch)
- Tooling list (ticketing, CVE monitoring, PGP)
- RACI matrix - PSIRT lead, engineering, regulatory, legal, comms

9. KPIs that prove the program is real

Mean time to acknowledge	Target: < 3 business days. Reviewer concern if > 7.
Mean time to triage	Target: < 10 business days. Trend over rolling 6 months.
Mean time to mitigate (Critical)	Target: < 30 days. Track P50 and P90.
Mean time to patch (Critical)	Target: < 60 days. Reviewer concern if > 90 without justification.
Reports received / quarter	Trend matters more than absolute number - growth shows trust.
Researcher repeat rate	Healthy programs see researchers come back. Indicator of credibility.

10. 60-day stand-up plan

- **Days 1-10:** Draft VDP policy, set up security@ + PGP, stand up intake form.

- **Days 10-25:** Build triage workflow in your ticketing/QMS system, define SLAs, train PSIRT team.
- **Days 25-40:** Run two tabletop exercises (Critical + Medium scenarios). Iterate.
- **Days 40-50:** Apply for CNA status (or document MITRE root path). Build advisory templates.
- **Days 50-60:** Soft-launch policy page, brief sales/support/legal, announce program.

Key takeaway: The fastest way to fail a postmarket review is to ship a CVD policy you don't actually run. Stand up the workflow first, validate with tabletops, then publish the policy.

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 CVD program working 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