BLUE GOAT CYBER
Medical Device Cybersecurity

MEDICAL DEVICE CYBERSECURITY GUIDE

Surgical Robot Section 524B Submission Guide

Prepare surgical robot Section 524B evidence: applicability, threat model, architecture views, SBOM, testing, postmarket plan, and eSTAR 7.1 cross-checks.

Reviewed 2026-11-10

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

IN BRIEF

A surgical robot Section 524B submission starts with a documented cyber device determination. When the statute applies, sponsors submit a postmarket vulnerability plan and an SBOM, maintain secure development processes, and make updates and patches available. The FDA's February 3, 2026 guidance recommends supporting evidence including threat modeling, security risk assessment, architecture views, testing, and labeling. Those records should describe the same robot configuration and keep clinical risk decisions with the manufacturer.

This page is a device-specific evidence crosswalk, not a new statutory interpretation or a completed client submission. The console, cart, imaging, service, and update examples are illustrative. Replace them with the actual product boundary and release records. For the engineering scenarios, read Surgical Robot Cybersecurity: Attack Paths and Submission Evidence.

Download the matching submission guide PDF.

Determine statutory applicability before preparing the package

Section 524B(a) covers submissions under the statutory provisions for 510(k), classification including De Novo, PMA, product development protocols, and humanitarian device exemptions when the device meets the cyber device definition. Document the actual pathway and applicable submission requirements with the regulatory team. IDE and Q-Submission interactions are not listed in Section 524B(a), although FDA cybersecurity guidance can be relevant to them.

All three Section 524B(c) conditions must be assessed:

1. The device includes software validated, installed, or authorized by the sponsor as a device or in a device.
2. The device has the ability to connect to the internet.
3. It contains technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

For a robot, examine direct and supported indirect connection paths through gateways, service tools, remote support, and update systems. A USB port or an Ethernet connector alone does not settle internet capability. Record how the actual system can connect, or why it cannot. Hospital isolation is a deployment control, not proof that the device lacks the ability.

Use the Section 524B statutory guide for the broader reference, and verify the statutory text when documenting applicability.

Separate binding duties from recommended evidence

The statute does not name every document recommended by the FDA. Keep that distinction visible in the package so an evidence checklist does not become an invented legal requirement.

Provision	Statutory duty	Robot-specific supporting evidence recommended under the guidance
524B(b)(1)	Submit a plan to monitor, identify, and address postmarket vulnerabilities and exploits, as appropriate in a reasonable time, including coordinated vulnerability disclosure and related procedures	Monitoring ownership, intake, affected-release analysis, clinical escalation, customer communication, and closure records
524B(b)(2)	Maintain secure design, development, and maintenance processes and procedures; make postmarket updates and patches available	SPDF/SSDLC records, threat model, security risk records, separate architecture views, security tests, and update/recovery evidence
524B(b)(2)(A)	Address known unacceptable vulnerabilities on a reasonably justified regular cycle	Justified update cadence, release assessment, supplier dependencies, installation conditions, and deployment tracking
524B(b)(2)(B)	Address critical vulnerabilities that could cause uncontrolled risks as soon as possible out of cycle	Escalation ownership, urgent remediation process, clinical coordination, and communication decisions
524B(b)(3)	Provide an SBOM including commercial, open-source, and off-the-shelf components	Release-specific machine-readable inventory, component relationships, support information, and separate vulnerability assessments
524B(b)(4)	Meet other requirements established through regulation	Check applicable regulations with the regulatory team; do not relabel guidance recommendations as regulations

KEY REQUIREMENT

Section 524B(b)(2) distinguishes regular-cycle treatment of known unacceptable vulnerabilities from out-of-cycle treatment of critical vulnerabilities that could cause uncontrolled risks. Neither this guide nor a template supplies a universal patch deadline.

The current supporting source is Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions, February 3, 2026. Guidance is nonbinding and permits alternative approaches that satisfy applicable legal requirements. The manufacturer's regulatory team should document any alternative and its evidence.

Establish the assessed configuration and document owners

Every artifact should identify the configuration it covers. Begin with device identifiers, intended use, supported operating environment, software and firmware releases, and related systems. Do not assume that all carts, instruments, or service tools in a device family share the same interfaces.

Preparation input	Device-specific question	Manufacturer owner to confirm
System boundary	Which console, cart, controllers, imaging functions, instruments, and related systems are included?	Systems engineering
Clinical states	What changes between setup, active procedure, maintenance, and recovery?	Clinical and safety owners
Release baseline	Which firmware, applications, dependencies, and build outputs were assessed?	Software/configuration management
Privilege model	Who can use clinical, service, administrative, and machine-to-machine functions?	Product security and engineering
Risk criteria	Which patient harms and acceptance criteria apply?	Manufacturer risk-management owner
Lifecycle support	Who monitors vulnerabilities, supplies patches, and approves field communication?	Product security, quality, and regulatory owners

Keep owner names, dates, requirement identifiers, and approval references in the manufacturer's controlled records. This public guide contains no client details or inferred project schedule.

Prepare a device-specific evidence crosswalk

The recommended evidence should explain actual controls and their test results. A list of document titles cannot establish how a threat is addressed.

Evidence record	Surgical robot content to prepare	Cross-check before filing
SPDF and secure development records	Security responsibilities, design requirements, supplier review, change control, defect handling, and lifecycle activities	Processes correspond to the manufacturer's QMS and assessed release
Threat model and Threat Table	Numbered entry points, data flows, trust boundaries, STRIDE classifications, prerequisites, controls, and traceability	No threat is treated as a confirmed finding without supporting evidence
Security risk assessment	Finding-specific exploitability and security effects, residual controls, and patient-safety links where supported	Manufacturer harm severity and risk decisions are referenced, not invented
Four architecture views	Global System, Multi-Patient Harm, Updateability/Patchability, and Security Use Case	Component identifiers and boundaries agree with the threat model
SBOM and vulnerability assessment	Console software, controller firmware, imaging, and in-scope support software with release mapping	Exact versions, coverage limitations, support level, and end-of-support information are visible

Evidence record	Surgical robot content to prepare	Cross-check before filing
Security test plan and report	Authorized interface tests, command-boundary checks, update authenticity, service privilege separation, and resource effects	Tested release, scope limits, unresolved findings, remediation, and retests are identifiable
Labeling and deployment instructions	Required network configuration, account roles, service access, updates, and clinically informed recovery instructions	Instructions match implemented behavior and manufacturer clinical review
Postmarket plan	Monitoring, disclosure, affected-device analysis, regular and urgent patching, communications, and closure	Owners and operating procedures exist beyond a future-tense promise

Threat-model diagrams and the Threat Table remain separate from the four security architecture views. A standalone Blue Goat threat-model engagement does not automatically include those architecture-view deliverables. See FDA medical device threat modeling and FDA cybersecurity architecture views for their distinct preparation tasks.

Keep SBOM scope aligned with the release and postmarket inventory

Identify how individual software inventories relate to the complete surgical platform. A console SBOM should not silently stand in for patient-side controller firmware or other in-scope systems. Record supplier-provided inventories, opaque packages, unresolved identifiers, and components excluded from coverage.

The FDA's February 3, 2026 guidance still cites NTIA 2021 minimum elements and recommends support level and end-of-support information. Blue Goat builds to CISA 2026 minimum elements plus those FDA support fields. Added CISA fields are not statutory FDA submission requirements. See the FDA SBOM requirements guide and CISA 2026 SBOM checklist.

Keep vulnerability assessment separate from inventory completeness. Assess whether each relevant issue affects the deployed version, configuration, and reachable code. Optional VEX can communicate that assessment when status-specific evidence exists; it is not a substitute for the required SBOM or device risk assessment.

Make the postmarket plan usable during and between procedures

The plan needs to distinguish a reported vulnerability from an active clinical incident. Define who assesses each, which release records identify affected installations, and what manufacturer-reviewed instructions apply to the device state.

For an illustrative service-account incident, the workflow might involve intake, credential containment, affected-configuration analysis, assessment of clinical access, customer communication, remediation, and confirmation of the resulting release. The actual sequence must reflect the manufacturer's architecture

and clinical review. It is not an instruction to disconnect an operating robot.

Document update authenticity, installation permissions, active-procedure restrictions, interrupted-update recovery, and support lifecycle decisions. Assign regular-cycle and urgent out-of-cycle decisions to responsible owners. Preserve risk rationale when immediate software remediation is unavailable, without assuming that a compensating control removes the statutory patching duty.

Use the postmarket cybersecurity readiness plan for detailed planning. A separately scoped tabletop can test organizational decisions; it does not validate clinical recovery or replace the manufacturer's approvals.

Cross-check the evidence before eSTAR preparation

Use the applicable current eSTAR 7.1 template for the submission pathway. Confirm its instructions and prompts, and reference the controlled evidence records rather than relying on a generic attachment location. This crosswalk does not claim that every listed pathway uses the same eSTAR workflow.

- [ ] Document the three-part cyber device determination and covered submission pathway.
- [ ] Identify the assessed robot release and all in-scope related systems.
- [ ] Match component names, interfaces, and boundaries across threat model and architecture views.
- [ ] Trace threats to actual requirements, implemented controls, security tests, and residual decisions.
- [ ] Reconcile SBOM releases with tested software and the vulnerability assessment.
- [ ] Identify unresolved findings, scope limitations, and manufacturer disposition.
- [ ] Include the postmarket plan with coordinated vulnerability disclosure and patching procedures.
- [ ] Confirm labeling, deployment, and recovery instructions match manufacturer-reviewed clinical behavior.
- [ ] Record approvals and verify each referenced document is included or otherwise supplied as instructed.

For document placement and preparation, use the eSTAR 7.1 submission checklist and FDA cybersecurity deliverables and eSTAR map. For dates, use the premarket submission planner with the manufacturer's actual project dates, not assumed turnaround times.

Frequently Asked Questions

Does this guide establish that a surgical robot submission meets Section 524B?

No. It organizes applicability questions, statutory duties, and supporting evidence for manufacturer review. A completed checklist does not establish legal compliance, clinical safety, or acceptance by the FDA. The regulatory team must assess the actual pathway and evidence, while the manufacturer retains risk, quality, and submission approvals.

Is a threat model enough without architecture views?

The threat model answers how threats arise across components and trust boundaries. The FDA guidance separately recommends four security architecture views addressing system context, multi-patient harm, patchability, and security use cases. The records should agree but remain identifiable as distinct evidence. Blue Goat scopes architecture views separately from standalone threat modeling.

Does the FDA require every CISA 2026 SBOM field?

No. Section 524B requires an SBOM including commercial, open-source, and off-the-shelf components. The FDA's February 3, 2026 guidance still cites NTIA 2021 and recommends additional support information. Blue Goat's CISA 2026 service baseline provides added inventory detail, but those added fields must not be presented as statutory FDA requirements.

Can the team assign patient harm from a CVSS score?

No. CVSS describes cybersecurity vulnerability characteristics and effects; its base score is not clinical harm severity. A supported path from compromise to a patient must be assessed with the manufacturer's ISO 14971 hazard analysis and acceptance criteria. Threat classifications and hypothetical attack paths do not supply a finding-specific score or safety decision.

What should teams do with missing supplier firmware inventories?

Record the affected package, release, supplier request, and coverage limitation. Determine how that gap affects vulnerability monitoring and the device assessment. Do not label the SBOM complete without evidence, and do not invent components. The manufacturer should review the gap and its disposition before assembling the submission records.

Discuss the surgical robot evidence scope

Bring the system boundary, planned submission pathway, release configuration, current risk records, and available supplier inventories. Blue Goat can scope FDA premarket cybersecurity support, independent medical device penetration testing, and postmarket cybersecurity support. The manufacturer owns clinical decisions and regulatory approvals.

Request a surgical robot cybersecurity consultation. If the FDA raises a cybersecurity question, we answer it at no extra cost until the cybersecurity portion is closed.

Sources

- Section 524B, 21 USC 360n-2
- FDA: Cybersecurity in Medical Devices, February 3, 2026
- FDA: Computer-Assisted Surgical Systems

About the author

Christian Espinosa, CISSP, Founder of Blue Goat Cyber. Christian works with medical device teams on cybersecurity evidence for premarket submissions and postmarket support. Read Christian's background.

Current web guide: bluegoatcyber.com/guides/surgical-robot-section-524b-submission

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.