BLUE GOAT CYBER
Medical Device Cybersecurity

MEDICAL DEVICE CYBERSECURITY GUIDE

FDA SBOM Requirements for Medical Devices

FDA SBOM requirements for cyber devices: Section 524B, recommended fields, support dates, submission evidence, and the separate role of optional VEX.

Reviewed 2026-11-05

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

IN BRIEF

Section 524B(b)(3) requires sponsors of covered cyber-device submissions to provide a software bill of materials, including commercial, open-source, and off-the-shelf software components. The FDA's February 3, 2026 guidance separately recommends machine-readable inventories, baseline component attributes, support status, and end-of-support dates. Industry-accepted formats are encouraged. No particular SPDX or CycloneDX version is prescribed in that passage. VEX is optional.

This guide helps medical device manufacturers separate the legal SBOM obligation from the FDA's documentation recommendations. It focuses on applicability and the evidence to assemble for a submission. For generation methods and the broader lifecycle, use SBOM for Medical Devices: The 2026 FDA Pillar Guide. For vulnerability-status communication, use the VEX document guide.

Which medical device submissions need an SBOM?

Section 524B applies to the submissions listed in subsection (a) for devices that meet the cyber-device definition in subsection (c). That definition has three conditions: software validated, installed, or authorized by the sponsor; the ability to connect to the internet; and technological characteristics authorized by the sponsor that could be vulnerable to cybersecurity threats. Assess the device against all three conditions rather than treating an SBOM obligation as universal.

For covered submissions, subsection (b)(3) requires the sponsor to provide an SBOM. The statutory text specifies commercial, open-source, and off-the-shelf components. It does not itself prescribe a file format, individual fields, or a periodic update interval. See 21 U.S.C. 360n-2, subsections (a), (b)(3), and (c).

The FDA's guidance also recommends software component documentation as part of cybersecurity risk management. A manufacturer should assess applicable documentation recommendations even when the statutory cyber-device definition does not apply. See the Section 524B guide for broader applicability planning.

Statutory duty versus FDA guidance recommendations

The primary guidance is Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions, February 3, 2026. Sections V.A.4(a), V.A.4(b), and VII.C.3 address SBOM scope, documentation, and the cyber-device obligation. Guidance recommendations are nonbinding unless a cited statute or regulation supplies a separate requirement.

Topic	What the source says	Source and status
Provide an SBOM	Include commercial, open-source, and off-the-shelf software components for covered cyber-device submissions	Section 524B(b)(3), statutory duty
Inventory scope	Include manufacturer-developed and third-party components and upstream dependencies	Guidance Section V.A.4(a), recommendation
Machine-readable delivery	Provide machine-readable SBOMs consistent with the baseline attributes referenced in the guidance	Guidance Section V.A.4(b), recommendation
Support information	Provide each component's support or maintenance status and end-of-support date, in the SBOM or an addendum	Guidance Section V.A.4(b), recommendation
Format selection	Industry-accepted formats are encouraged	Guidance Section V.A.4(b), recommendation
Lifecycle maintenance	Maintain the SBOM or equivalent capability in configuration management and update it as marketed devices change	Guidance Section V.A.4(a), recommendation

What fields should the SBOM contain?

The guidance references the NTIA baseline attributes. The NTIA 2021 Minimum Elements for an SBOM identify supplier name, component name, component version, other unique identifiers, dependency relationships, the author of the SBOM data, and a timestamp. These are the baseline referenced by the guidance, not an FDA-specific SBOM schema. A newer general SBOM specification does not automatically amend the FDA guidance or statute.

Attribute	Evidence to collect	Review question
Supplier and component name	Supplier records and consistent component names	Can another reviewer identify the component without guessing?
Component version	Resolved versions from the build or delivered artifact	Does the version match the submitted product?
Unique identifiers	Available ecosystem or supplier identifiers	Can vulnerability matching distinguish similarly named packages?
Dependency relationships	Direct and upstream dependency records	Are dependencies represented, and are known gaps explained?
SBOM data author and timestamp	Identified data author and generation record	Who produced this inventory, and when?
Support or maintenance status	Supplier evidence or documented investigation	Is the component maintained, no longer maintained, or abandoned?

Attribute	Evidence to collect	Review question
End-of-support date	Confirmed supplier date or an explicit unknown	Does the record distinguish confirmed dates from unresolved information?

Component identifiers such as PURL and CPE can support vulnerability matching. Their usefulness depends on the ecosystem and advisory source. Do not invent identifiers to fill a field. See the CPE vs PURL guide.

How should manufacturers handle unknown support dates?

Request information from the supplier and preserve the response or the unanswered request. Mark unavailable information as unknown, describe the affected components, and explain how the uncertainty is addressed in risk and support planning. Do not infer an end-of-support date from a component's release date or the manufacturer's planned device life.

Section V.A.4(b) recommends a justification when a manufacturer cannot provide SBOM information. That recommendation is not an exemption from the statutory SBOM duty. Support-status and end-of-support information may be delivered in a separate addendum linked to the component records.

Does the FDA require SPDX or CycloneDX?

The cited guidance encourages industry-accepted formats. It does not prescribe SPDX, CycloneDX, a particular serialization, or a minimum format version. Choose a machine-readable format that your tooling and intended recipients can use, then validate the file against that format's schema.

Blue Goat uses SPDX as its default delivery format. That is a delivery practice, not an FDA mandate. For format differences, use CycloneDX vs. SPDX for Medical Devices.

What evidence should accompany a submission SBOM?

Use a release-specific evidence package rather than an inventory disconnected from the product being submitted. The following is a practical review checklist, not a prescribed FDA attachment naming scheme:

- Identify the device, software release, and included system elements.
- Record the source, build, binary, and supplier evidence used to establish component coverage.
- Include the machine-readable SBOM and any linked support-information addendum.
- Explain excluded scope, unresolved composition gaps, and unavailable component information.
- Retain generation tool versions, configuration, schema validation results, and review records.
- Connect known vulnerabilities to product-specific assessment, controls, remediation, and unresolved-anomaly records where applicable.

- Reference the inventory and associated evidence in the applicable submission documentation. Use the current eSTAR prompts for your pathway rather than an invented attachment slot.

An SBOM lists composition. It is not proof that a component is free of vulnerabilities. The guidance separately recommends identification of known vulnerabilities, risk assessment, and controls. See SBOM Vulnerability Management for Medical Devices.

Can VEX replace the SBOM?

No. VEX communicates an assessment of vulnerability status for identified product versions. It is optional and the February 3, 2026 guidance does not mention it. Neither a not_affected label nor a scanner's lack of matches replaces the underlying assessment.

When VEX is used, connect statements to the affected product versions and retain the evidence supporting the status. Keep the SBOM, vulnerability assessment, and manufacturer safety and risk decisions distinct. The VEX document guide explains the statuses and their supporting evidence.

Maintaining the inventory after submission

The FDA recommends maintaining the SBOM or equivalent capability within configuration management and updating it as marketed devices change. Section 524B separately establishes postmarket vulnerability-management and update-process duties for covered cyber devices. The SBOM clause does not set a universal monthly or quarterly refresh deadline.

As a practical release-control measure, retain inventories associated with released builds and review composition when software changes. New vulnerability information can require reassessment even when composition is unchanged. Manufacturer review determines risk acceptance, fixes, and release decisions. See postmarket SBOM maintenance.

How Blue Goat approaches SBOM evidence

Blue Goat reconciles available source, build, binary, and supplier evidence within the agreed scope. Delivery records include tool versions and configuration, component enrichment, and second-person peer review. Unknown supplier dates remain unknown pending supplier response. The manufacturer retains configuration management, fixes, clinical severity evidence, risk acceptance, and release ownership.

For scoped, fixed-fee support, explore medical device SBOM services. For a broader submission engagement, explore FDA premarket cybersecurity services. Confidential material is handled under the agreed NDA and statement of work.

FAQ

Is an SBOM required for every medical device?

Section 524B requires an SBOM for covered submissions involving a device that meets its cyber-device definition. Assess applicability rather than treating every medical device as covered. The FDA guidance separately recommends software component documentation as part of cybersecurity risk management.

What components must a cyber-device SBOM include?

The statute specifies commercial, open-source, and off-the-shelf software components. The guidance describes inventory coverage that includes manufacturer-developed and third-party components and upstream dependencies.

Does the FDA require a machine-readable SBOM?

The February 3, 2026 guidance recommends machine-readable SBOMs. Section 524B(b)(3) requires the SBOM but does not itself specify machine-readable delivery. Keep the statutory obligation and guidance recommendation distinct.

Does the FDA mandate SPDX or CycloneDX?

No particular format or minimum version is prescribed in the cited guidance. Industry-accepted formats are encouraged. Blue Goat's SPDX default is a delivery practice, not an FDA mandate.

Are support status and end-of-support dates part of the recommended evidence?

Yes. Section V.A.4(b) recommends both for each component. They may be included in the SBOM or a separate addendum. Document unavailable information and the justification without inventing supplier dates.

Is VEX required alongside the SBOM?

No. The February 3, 2026 guidance does not mention VEX. It can supplement vulnerability-status communication but cannot replace the SBOM, vulnerability assessment, or manufacturer risk decisions.

How often must the SBOM be updated?

The guidance recommends regular updates reflecting changes to marketed devices. The SBOM clause does not prescribe a universal monthly or quarterly interval. Define release-linked maintenance and vulnerability reassessment in the manufacturer's processes.

Sources

- 21 U.S.C. 360n-2: Ensuring cybersecurity of devices, Section 524B, especially subsections (a), (b)(3), and (c).
- FDA premarket cybersecurity guidance, February 3, 2026, Sections V.A.4(a), V.A.4(b), and VII.C.3.
- NTIA Minimum Elements for a Software Bill of Materials, 2021, the baseline referenced by the FDA guidance.

Download the guide

Download FDA SBOM Requirements for Medical Devices (PDF).

About the author

Christian Espinosa, Founder, Blue Goat. Christian leads a team focused on medical device cybersecurity. Read more about Christian.

Current web guide: bluegoatcyber.com/guides/fda-sbom-requirements-medical-devices

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.