IntuitionLabs

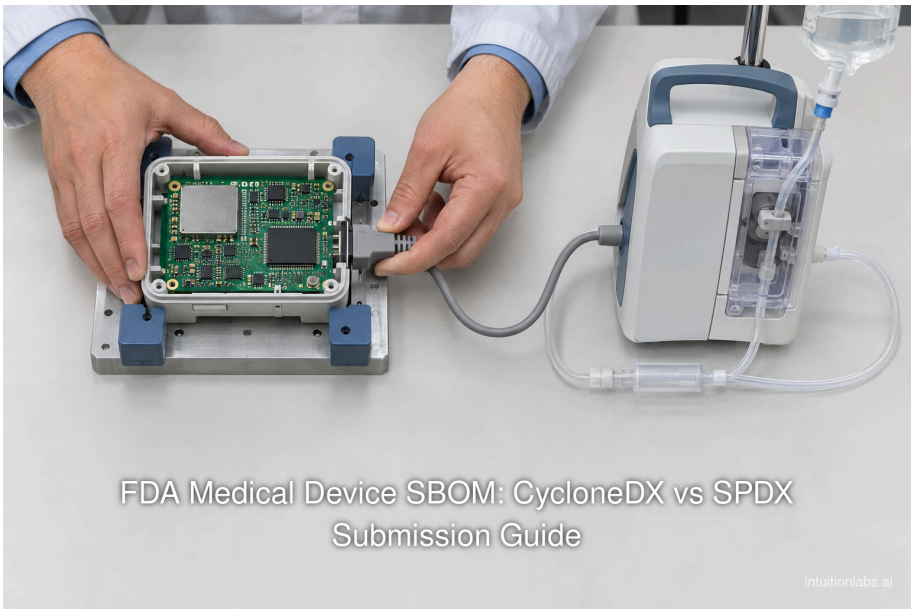
INTUITIONLABS / RESEARCH & PRACTICAL GUIDANCE

FDA Medical Device SBOM: CycloneDX vs SPDX Submission Guide

> Build practical AI for pharma and biotech with IntuitionLabs. We help life-science teams turn complex information and workflows into useful software, governed knowledge systems and AI tools.

Published by IntuitionLabs · 2026-11-11 · fda medical device sbom · cyclonedx vs spdx · sbom format for fda submission · section 524b · ntia minimum elements · vex · medical device cybersecurity · estar

Original article: https://intuitionlabs.ai/articles/fda-medical-device-sbom-cyclonedx-vs-spdx



In this article

1. Executive Summary
2. Introduction and Background
3. Regulatory Basis: Law, Guidance and Recommendation
4. What FDA and IMDRF Expect in and around an SBOM
5. CycloneDX: Capabilities, Adoption, Strengths and Limitations
6. SPDX: Capabilities, Adoption, Strengths and Limitations
7. Feature Comparison and Field-Level Crosswalk
8. Pipeline Architecture: From Build to eSTAR
9. VEX and Vulnerability Triage
10. Lifecycle Management and Change Control
11. Performance and Benchmarks: What the Evidence Shows About SBOM Quality
12. Data Analysis and Evidence
13. Case Studies and Real-World Examples
14. Implications and Future Directions
15. Frequently Asked Questions (FAQs)
16. Conclusion

Executive Summary

For a medical device that qualifies as a "cyber device," a software bill of materials (SBOM) is not optional. Section 524B(b)(3) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) requires the sponsor to provide "a software bill of materials, including commercial, open-source, and off-the-shelf software components" (www.law.cornell.edu). FDA's February 2026 final premarket cybersecurity guidance restates that an SBOM is required for cyber devices (www.fda.gov), and FDA says an electronic Submission Template And Resource (eSTAR) file goes on Technical Screening hold if its Cybersecurity section lacks accurate responses and relevant attachments (www.fda.gov). The guidance carries an issue date of February 3, 2026 (the PDF header date) (www.fda.gov), while FDA's cybersecurity page lists the revision under a February 2, 2026 entry; this article refers to the guidance simply as the February 2026 guidance (www.fda.gov).

The statute and the guidance do not choose a file format. The guidance recommends machine-readable SBOMs consistent with the National Telecommunications and Information Administration (NTIA) minimum elements, also called "baseline attributes" (www.fda.gov), and refers to "industry-accepted formats" (www.fda.gov). As of November 2026, the guidance text does not name SPDX (Software Package Data Exchange) or CycloneDX. The International Medical Device Regulators Forum (IMDRF) document N73 lists CycloneDX, SPDX and SWID (software identification tags) as prominent formats without ranking them (www.imdrf.org), and the 2026 minimum elements from the Cybersecurity and Infrastructure Security Agency (CISA) name SPDX and CycloneDX as the two widely used formats (www.cisa.gov). The format decision is an engineering decision, not a legal one.

The formats differ in ways that matter for devices. CycloneDX 1.7, standardized as ECMA-424 (ecma-international.org), carries vulnerability analysis in the same schema (cyclonedx.org). SPDX 2.3 has a native field for the end of a supplier's support period (spdx.github.io), which maps to FDA's request for component support level and end-of-support date (www.fda.gov), and SPDX 3.0.1 adds a Security profile for Vulnerability Exploitability eXchange (VEX) statements (spdx.github.io). Neither format proves compliance, and FDA states that VEX does not replace the vulnerability assessment it recommends (www.fda.gov).

Data quality is the larger risk. A preprint comparing six generators on 3,287 repositories reported inter-tool consistency for package detection as low as 7.84% to 12.77% (arxiv.org), and 62% of respondents to a 2026 European Union Agency for Cybersecurity (ENISA) survey named SBOM completeness a technical challenge (www.enisa.europa.eu). This report recommends one canonical format per device line, generation in the build, supplier merge with provenance, automated quality gates, signing, archiving, and a new SBOM for every software change, consistent with IMDRF N73 (www.imdrf.org). It is analysis, not legal advice.

Introduction and Background

A software bill of materials is a formal inventory of software components and dependencies, with their information and hierarchical relationships; FDA's guidance adopts this definition from NTIA (www.fda.gov). For product security teams the practical question is which representation to use, how to produce it reliably for every release, how to take supplier data in, how to package evidence for FDA, and how to keep the artifact accurate after the device ships.

This report serves product security, regulatory affairs and quality teams. Every factual statement is cited to a third-party regulator, standards body, project documentation or research source, and all dates are stated as of November 2026.

The report separates three layers that are often blurred: what the law requires, what FDA recommends in guidance, and what this report recommends as implementation practice.

Regulatory Basis: Law, Guidance and Recommendation

What section 524B requires

Section 524B was added by the Food and Drug Omnibus Reform Act (FDORA) and took effect 90 days after December 29, 2022 (www.law.cornell.edu). A "cyber device" includes software validated, installed or authorized by the sponsor (www.law.cornell.edu), has the ability to connect to the internet (www.law.cornell.edu), and contains technological characteristics that could be vulnerable to cybersecurity threats (www.law.cornell.edu).

For a cyber device the sponsor must run a postmarket plan that monitors, identifies and addresses vulnerabilities, including coordinated vulnerability disclosure (www.law.cornell.edu); provide updates and patches for known unacceptable vulnerabilities on a reasonably justified regular cycle (www.law.cornell.edu) and out of cycle for critical vulnerabilities that could cause uncontrolled risks (www.law.cornell.edu); and provide the SBOM (www.law.cornell.edu). The Secretary may exempt devices or categories of devices (www.law.cornell.edu). None of these provisions names an SBOM format or enumerates SBOM fields.

Which submissions are covered

FDA's FAQ lists covered pathways including Product Development Protocol (PDP), De Novo and Humanitarian Device Exemption (HDE) requests (www.fda.gov), alongside 510(k) and premarket approval (PMA) submissions. The requirements do not apply to a submission made before March 29, 2023, but a new submission for a change to a previously authorized cyber device is in scope.

What the February 2026 guidance adds

The guidance applies to devices with cybersecurity considerations, including but not limited to devices with software, firmware or programmable logic (www.fda.gov); cyber devices are a subset. It was revised to align with the amendments to 21 CFR Part 820, the Quality Management System Regulation (QMSR) (www.fda.gov), and supersedes the version issued June 27, 2025 (www.fda.gov). Teams should compare the 2025 and 2026 texts themselves to identify what changed.

The guidance distinguishes what is required from what is recommended. The SBOM is required by statute for cyber devices, and Section VII.C.3 recommends that it contain the information described in Section V.A.4.b (www.fda.gov). The existence of an SBOM is therefore a statutory matter, while field content and format are matters of FDA recommendation that reviewers assess for adequacy.

Table 1 summarizes the layers so that teams label each requirement correctly in design history documentation.

Layer	Source	What it says about SBOMs	Status
Statute	FD&C Act 524B(b)(3)	Provide an SBOM including commercial, open-source and off-the-shelf components	Binding for cyber devices
FDA guidance	Premarket cybersecurity guidance, Section V.A.4	Machine-readable, NTIA-consistent, plus level of support and end-of-support date (www.fda.gov)	Recommendation; adequacy reviewed
FDA FAQ	Cybersecurity FAQ	Technical Screening hold if the eSTAR Cybersecurity section lacks accurate responses and attachments (www.fda.gov)	Describes FDA process
International principles	IMDRF N73	Baseline elements follow NTIA; formats named without ranking (www.imdrf.org)	Non-binding principles
Implementation	This report	Single canonical format, continuous integration (CI) generation, quality gates	Analyst recommendation

No binding layer prescribes CycloneDX or SPDX. Teams should document the format choice as a design decision with a rationale and should not describe either format as FDA-required or FDA-endorsed in submission text.

What FDA and IMDRF Expect in and around an SBOM

FDA Section V.A.4

FDA describes a robust SBOM as covering manufacturer-developed and third-party components with their upstream dependencies (www.fda.gov). The SBOM should be part of configuration management and be regularly updated to reflect software changes in marketed devices (www.fda.gov). Section V.A.4(b)

recommends two attributes beyond the NTIA elements for each component: the level of support from the component manufacturer (www.fda.gov) and the component end-of-support date. If a manufacturer cannot provide SBOM information, FDA recommends a justification in the submission (www.fda.gov).

The SBOM sits inside a connected body of evidence. The security risk management report should include the SBOM, component support information and vulnerability assessments (www.fda.gov), with traceability among the threat model, risk assessment, SBOM and testing documentation (www.fda.gov). FDA asks for identification of known vulnerabilities, including those in the CISA Known Exploited Vulnerabilities (KEV) catalog (www.fda.gov), and a safety and security risk assessment of each (www.fda.gov). Labeling should make machine-readable SBOM information available to users, and manufacturers should plan for updating or replacing third-party software whose support ends (www.fda.gov).

IMDRF N73 principles

IMDRF published N73, "Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity," as a final document in April 2023 (www.imdrf.org). It recommends that a baseline SBOM follow NTIA (www.imdrf.org), defines the author element as the entity that produced the SBOM file (www.imdrf.org), and recommends a component hash (www.imdrf.org). It treats the end-of-support date as supplemental lifecycle information (www.imdrf.org) and recommends mapping device SBOMs to a unique device identifier so an SBOM matches the right device and version (www.imdrf.org). It sets the change rule that drives operations: any event that causes the device software to change should result in a new SBOM (www.imdrf.org). It also notes that an SBOM does not explicitly state whether a component has a vulnerability (www.imdrf.org).

NTIA 2021 and CISA 2026 minimum elements

NTIA's 2021 minimum elements define seven data fields, including other unique identifiers, dependency relationship and author of SBOM data (www.ntia.doc.gov), and name SPDX, CycloneDX and SWID tags as formats (www.ntia.doc.gov). NTIA also requires authors to identify "known unknowns" where the dependency graph is incomplete (www.ntia.doc.gov).

The broader U.S. baseline has moved. CISA opened comment on an updated draft in August 2025 (www.cisa.gov), and the final 2026 Minimum Elements, published July 29, 2026, update and replace the NTIA elements (www.cisa.gov). The final adds requirements for component hash, license, SBOM tool name and SBOM generation context (content.govdelivery.com), renames the supplier concept "component producer" because of ambiguity around distributors (www.cisa.gov), and says each software version or update should have an associated SBOM (www.cisa.gov).

FDA's current text still cites the NTIA baseline, and the 2026 CISA fields are not presented there as a requirement. Treating the CISA additions as a superset is an analyst inference, not an FDA position.

CycloneDX: Capabilities, Adoption, Strengths and Limitations

Capabilities

CycloneDX is an OWASP (Open Worldwide Application Security Project) full-stack bill of materials standard (owasp.org). Version 1.7 was announced on October 21, 2025 (cyclonedx.org), and ECMA-424 now defines v1.7, following ratification of v1.6 in June 2024 (cyclonedx.org). It can represent software, hardware devices, machine learning models, source code and configurations (cyclonedx.org). As of November 2026, the CycloneDX Tool Center listed 337 tools (cyclonedx.org). Serializations are JSON, XML and Protocol Buffers (cyclonedx.org), and the JSON Schema is the reference implementation (github.com).

Several native constructs matter for devices. A hardware device containing firmware should include a component for the physical hardware itself (cyclonedx.org). The dependency graph represents direct and transitive relationships (cyclonedx.org). Compositions carry a completeness aggregate (cyclonedx.org). Metadata lifecycles record when data was captured (cyclonedx.org), including post-build for information obtained after a build completes (cyclonedx.org). Component identity can use package URLs (purl) (cyclonedx.org).

Adoption

ENISA's 2026 survey of 334 respondents, mostly European organizations (www.enisa.europa.eu), found 44% using CycloneDX and 29% using SPDX (www.enisa.europa.eu), with 17% still on a proprietary format (www.enisa.europa.eu). These are respondent usage shares, not market share, and the survey is not specific to medical devices. A preprint comparing 108 open-source and 62 proprietary tools advertised for SPDX and CycloneDX (arxiv.org) reported that CycloneDX projects show higher developer engagement and certain community-health metrics (arxiv.org).

Strengths and limitations

Documented strengths include native vulnerability analysis states and justifications (cyclonedx.org), BOM-Link for connecting separate BOM and VEX documents (cyclonedx.org), enveloped signing (cyclonedx.org), and name-value properties as an extension mechanism (cyclonedx.org).

Limitations are practical. CycloneDX publishes a property taxonomy that defines `cdx:lifecycle:milestone:endOfSupport` for the end-of-support date. It defines no support-level property, so teams would document FDA's level-of-support attribute as a custom property under an agreed naming convention (analyst assessment). Mapping documents should be checked against the schema version in use, because field names change between releases.

SPDX: Capabilities, Adoption, Strengths and Limitations

Capabilities

SPDX is an open source project hosted by the Linux Foundation (spdx.dev), and is described as an international open standard, ISO/IEC 5962:2021 (spdx.dev); that edition corresponds to SPDX 2.2.1 (spdx.github.io), which predates 2.3. The 2.3.1 text states that the latest edition is 3.0.1, from December 2024

(spdx.github.io), and that 2.3.1 adds no new fields (spdx.github.io). A 3.1 release candidate existed but no general availability release was found when checked (github.com).

SPDX 2.x supports several serializations and requires interoperability among them (spdx.github.io). SPDX 3.0.1 is RDF-based (spdx.github.io), and conformance involves structural plus semantic validation (spdx.github.io). It defines nine profiles, of which only Core is mandatory (spdx.github.io).

Device-relevant SPDX 2.3 fields include a package supplier that must be an organization or recognized author and not a website (spdx.github.io), checksums for unique identification (spdx.github.io), and a primary purpose value for firmware (spdx.github.io). The 2.3 valid-until date records the end of the supplier's support period (spdx.github.io). In 3.0.1 the equivalent is validUntilTime (spdx.github.io) with a support-level vocabulary that includes endOfSupport (spdx.github.io), and deviceDriver joins the purpose vocabulary (spdx.github.io).

Adoption

SPDX is widely used in embedded builds. The Yocto Project's OpenEmbedded build system generates SPDX SBOM information by default (docs.yoctoproject.org), Zephyr's SBOM command defaults to SPDX 2.3 and flags SPDX 3.1 support as experimental (docs.zephyrproject.org), and Microsoft's sbom-tool defaults to SPDX 2.2 for generation (github.com).

Strengths and limitations

Strengths include the ISO lineage of the 2.2.1 edition, native license and checksum fields, a mature relationship model such as DEPENDS_ON (spdx.github.io), SPDX-lite described as satisfying NTIA minimum SBOM element requirements (spdx.dev), and an NTIA mapping in the 2.3.1 text stating the format contains fields able to address each NTIA minimum element (spdx.github.io). The same text says it addresses only some of the 2026 CISA fields (spdx.github.io) and has no field for the SBOM author signature (spdx.github.io), so signatures must be carried externally. SPDX 3.0.1 adds relationship completeness values (spdx.github.io) and SBOM type values for generation context (spdx.github.io).

Tool support is split across versions. An SBOM aggregation tool may support only an older release, as sbom-tool's aggregation does (github.com), and the SPDX NTIA conformance checker advertises versions 2.2, 2.3 and 3.0 (github.com). Teams choosing SPDX 3.0.1 should confirm that downstream consumers read it.

Feature Comparison and Field-Level Crosswalk

Decision matrix

Table 2 compares the representations on criteria that usually decide a device program's choice. Where a capability was not found in the reviewed sections, the cell says so.

Criterion	CycloneDX 1.7	SPDX 2.3.1 / 3.0.1
Standardization	ECMA-424 defines v1.7	ISO/IEC 5962:2021 is the 2.2.1 edition; 3.0.1 is the latest edition

Criterion	CycloneDX 1.7	SPDX 2.3.1 / 3.0.1
Serialization	JSON, XML, protobuf	2.x multiple formats; 3.0.1 JSON-LD and RDF forms
Firmware and hardware	Firmware and device component types	FIRMWARE and DEVICE purposes in 2.3; deviceDriver added in 3.0.1
Completeness assertion	Composition aggregate values	Relationship completeness in 3.0.1
End-of-support data	No dedicated schema field; `cdx:lifecycle:milestone:endOfSupport` in the property taxonomy; support level as a custom property	validUntilDate in 2.3; supportLevel and validUntilTime in 3.0.1
VEX in same schema	Native analysis states	3.0.1 Security profile; 2.3 relies on external references (spdx.github.io)
Signing	JSON Signature Format (JSF) and XML signature options	No SBOM author signature field in 2.3.1
Generators and embedded builds	Polyglot generator and CLI ecosystem (github.com)	Yocto and Zephyr SPDX generation
Conversion	CLI converts among CycloneDX serializations and SPDX JSON 2.3 (github.com)	Conversion possible; field loss must be tested

The matrix suggests a decision rule, not a winner. Programs that build with Yocto or Zephyr, or need an ISO-lineage artifact, have a natural SPDX path; programs with polyglot application stacks and integrated VEX have a natural CycloneDX path. Many manufacturers will keep one canonical format for the submission and convert for customers who request the other.

Field-level crosswalk

Table 3 maps each FDA, IMDRF and CISA expectation to fields in both formats. The status column is an analyst assessment of whether the field is native, needs an extension or property, or belongs in a supporting document submitted next to the SBOM.

Expectation (source)	CycloneDX 1.7 field	SPDX field	Status
SBOM author (NTIA, IMDRF)	metadata.authors	creationInfo.creators (spdx.github.io)	Native in both
Timestamp (NTIA)	metadata.timestamp	created (spdx.github.io)	Native in both
Supplier or producer (CISA 2026)	components[].supplier	supplier	Native in both
Name and version (NTIA)	components[].name, version	name, versionInfo (optional in 2.3 (spdx.github.io))	Native in both
Unique identifier (IMDRF)	purl, cpe, bom-ref	externalRefs; packageUrl in 3.0.1 (spdx.github.io)	Native in both

Expectation (source)	CycloneDX 1.7 field	SPDX field	Status
Dependency relationship	dependencies[]	DEPENDS_ON	Native in both
Component hash (IMDRF, CISA 2026)	hashes[]	checksums	Native in both
License (CISA 2026) (www.cisa.gov)	licenses[]	licenseConcluded, licenseDeclared (spdx.github.io)	Native in both
Generation context (CISA 2026) (www.cisa.gov)	metadata.lifecycles	sbomType in 3.0.1; creator comment in 2.3	Native in CycloneDX and 3.0.1; partial in 2.3
Tool name and version	metadata.tools	Tool creator entry	Native in both
SBOM signature	JSON Signature Format	None in 2.3.1	Native in CycloneDX; external for SPDX 2.3
Level of support (FDA)	Property extension	supportLevel in 3.0.1	Extension in CycloneDX and 2.3
End-of-support date (FDA)	Property, taxonomy-defined (`cdx:lifecycle:milestone:endOfSupport`)	validUntilDate	Native in SPDX; taxonomy-defined property in CycloneDX
Known vulnerabilities and assessment (FDA)	vulnerabilities[] analysis	Security profile	Native in CycloneDX and 3.0.1; supporting document for 2.3
KEV status (FDA)	Triage record or property	ExploitCatalog relationship (spdx.github.io)	Native in 3.0.1; supporting record otherwise
Device identifier mapping (IMDRF)	Property on metadata.component	externalRef or externalIdentifier	Extension
Justification when data is unavailable (FDA)	Supporting document	Supporting document	Supporting document
Traceability to threat model (FDA)	Supporting document	Supporting document	Supporting document

The core NTIA and CISA fields are native in both formats. FDA's two support attributes and IMDRF's device identifier mapping are where either format needs a convention. The most defensible approach is a written SBOM profile: a short, version-controlled specification of the fields, properties and naming conventions every SBOM in the product line will contain.

Pipeline Architecture: From Build to eSTAR

This pattern is derived from the cited sources and is not an FDA-prescribed process.

Generate, normalize and merge

- **Build and generate.** Produce an SBOM at build time from lockfiles, the build graph and image contents; software composition analysis tools can generate an SBOM (healthsectorcouncil.org). Yocto builds emit SPDX information by default, and general-purpose scanners such as Trivy document both CycloneDX and SPDX output (trivy.dev).
- **Normalize.** Convert to the canonical format and normalize names, versions and supplier strings. FDA's FAQ describes the advantages of standard nomenclature and formats for consistent data (www.fda.gov).
- **Add post-build evidence.** Scan the final image to catch components that manifests miss and record the generation context.
- **Collect supplier SBOMs** for purchased modules and third-party libraries. The Health Sector Coordinating Council's joint security plan recommends that suppliers provide an updated SBOM for every release (healthsectorcouncil.org) and includes sample contract language to maintain an SBOM for all product versions (healthsectorcouncil.org).
- **Merge with provenance.** Preserve which statements came from the supplier and which from your own scan. BOM-Link can reference another BOM's components, and the CycloneDX command-line tool lists merging among its functions (cyclonedx.org).
- **Record unresolved components** explicitly. NTIA's "known unknowns" practice maps to CycloneDX completeness aggregates.

Quality gates

- **Schema validation.** Reject any SBOM that fails its schema. The CycloneDX command-line tool returns a non-zero exit code on invalid BOMs (github.com), and the SPDX Python tools validate against v2.2 and v2.3 (github.com).
- **Minimum-element conformance.** The SPDX NTIA conformance checker validates against NTIA, CISA and other minimum element requirements (github.com).
- **Completeness, age and support-status checks.** Apply the metrics defined in the Data Analysis section, and fail the build if a component lacks a support level or end-of-support entry.

Sign, archive and hand off to eSTAR

- **Sign.** CycloneDX supports enveloped signing, Syft can create signed in-toto attestations (github.com), and Sigstore's Cosign signs attestation payloads using the Dead Simple Signing Envelope (DSSE) specification (docs.sigstore.dev). Sigstore documentation notes that SBOM predicate types are not recommended (docs.sigstore.dev), and suggests attesting a pointer plus a hash instead. A software attestation is an authenticated statement about software artifacts (slsa.dev).
- **Archive.** Store the SBOM, build identifier, source revision, generator version and validation report in the design history file.
- **Attach.** The 510(k) eSTAR guidance lists a Cybersecurity/Interoperability section for applicable assessment information (www.fda.gov), and eSTAR is mandatory for 510(k) and De Novo submissions to the Center for Devices and Radiological Health (CDRH) or the Center for Biologics Evaluation and Research (CBER) unless exempted (www.fda.gov).

- **Package.** Include the SBOM in the canonical format, the supporting documents from Table 3, and the traceability evidence. FDA lists SBOM, vulnerability assessment and software support documentation among its premarket considerations.
- **Confirm the template.** Exact eSTAR question wording and attachment slots change with template versions, so confirm them against the current template.

VEX and Vulnerability Triage

Why an SBOM alone is not exploitability analysis

An SBOM states what is in the device, not whether a component is vulnerable (www.imdrf.org), and not whether a vulnerability is exploitable in the device's configuration. CISA describes VEX as indicating the status of a software product or component with respect to a vulnerability (www.cisa.gov), and IMDRF defines it as a machine-readable assertion about the status of a vulnerability in specific products (www.imdrf.org). FDA is explicit that VEX does not provide sufficient information on its own to replace the recommended vulnerability assessment (www.fda.gov).

VEX formats

CISA's minimum requirements identify CSAF, CycloneDX and OpenVEX as formats that can carry VEX (www.cisa.gov), and note that CSAF and CycloneDX carry information beyond VEX requirements (www.cisa.gov). OpenVEX describes itself as lightweight and embeddable while meeting the CISA requirements (github.com). The OASIS Common Security Advisory Framework (CSAF) version 2.1 defines a VEX profile (docs.oasis-open.org) but was still a committee specification draft on October 21, 2026 (docs.oasis-open.org). CycloneDX treats VEX as a subset of its vulnerability disclosure content (cyclonedx.org) and recommends decoupling VEX from the SBOM so it can change without reissuing the BOM (cyclonedx.org). SPDX 3.0.1 expresses not-affected through a relationship restricted to the doesNotAffect type (spdx.github.io). The CISA document is not official CISA policy (www.cisa.gov). For a manufacturer, VEX is a communication layer on top of the internal vulnerability assessment, not a replacement for it.

Triage workflow

1. **Match** components to vulnerability data using purl and CPE identifiers.
2. **Prioritize** with exploitation signals. CISA advises using the KEV catalog as an input to prioritization (www.cisa.gov); it showed 1,779 entries as of November 2026 (www.cisa.gov). The Exploit Prediction Scoring System (EPSS) estimates the probability that a published vulnerability will be exploited in the wild in the next 30 days (www.first.org), and a score of 0.05 corresponds to a 5% empirical rate (www.first.org).
3. **Assess** device-specific exploitability and patient-safety impact. A 2,414-repository study found that downstream vulnerability scanners produced a very high false-positive rate in its case study (arxiv.org), and that function call analysis pruned 61.9% of those false alarms (arxiv.org).
4. **Decide** status and justification. CISA lists justification values for not-affected status (www.cisa.gov), treats them as assertions a consumer may accept or reject (www.cisa.gov), and requires a justification or impact statement (www.cisa.gov). OpenVEX discourages free-text impact statements because they

break automation (github.com).

5. **Classify** risk as controlled or uncontrolled using FDA's postmarket definition of uncontrolled risk (www.fda.gov), then route to patch, compensating control or customer notification.

Lifecycle Management and Change Control

Versioning and postmarket duties

Three sources align on the core rule: IMDRF N73 says any change to device software should result in a new SBOM, the 2026 CISA elements say each version or update should have an associated SBOM, and FDA says the SBOM should be regularly updated to reflect software changes in marketed devices.

FDA's postmarket guidance, issued December 28, 2016 (www.fda.gov), recommends monitoring third-party software components for new vulnerabilities throughout the lifecycle (www.fda.gov). As of November 2026, confirm on FDA's cybersecurity page whether a later version has replaced it. The guidance also sets conditions for its enforcement-discretion path on uncontrolled risks; read the guidance text itself, and do not treat any timeline as removing reporting obligations under 21 CFR Part 806. The Health Information Sharing and Analysis Center (Health-ISAC) describes machine-readable, standardized SBOMs as enabling automated analysis and integration into cybersecurity workflows (health-isac.org). FDA recommends submitting the cybersecurity management plan, including its patch timeline, with the premarket submission (www.fda.gov).

Change-impact matrix

Table 4 shows a change-impact flow using hypothetical components. It illustrates the data a product security team must join: component, vulnerability, affected device versions, submissions and field units, and decision.

Trigger	Vulnerability and status	Device versions affected	Submissions and field units	Decision path
Library "examplelib" 1.4.2 to 1.4.3 (Hypothetical Example)	New advisory lists 1.4.2 as affected; KEV status checked	Firmware 3.2.0 and 3.2.1 in the SBOM archive	Cleared submissions and field units by serial range from the device identifier mapping	Assess exploitability, classify controlled or uncontrolled, patch on cycle or out of cycle
Component reaches end of support (Hypothetical Example)	Supplier issues no new advisories	All versions containing the component	Labeling should disclose end-of-support information	Replace the component or document the pre-established transition process
Supplier replaces a proprietary module (Hypothetical Example)	Supplier SBOM changes the component list	Next release only	Change assessment decides whether a new submission is needed	New SBOM; supplier SBOM refreshed

The matrix is useful only if the SBOM archive can answer "which shipped versions contain component X at version Y" in seconds. That requires indexing every archived SBOM by device version and unique device identifier in a monitoring platform. Dependency-Track, for example, documents consuming and producing CycloneDX VEX (docs.dependencytrack.org) and re-analyzing its portfolio on a schedule

(dependencytrack.github.io). The platform choice is the manufacturer's; the join is the requirement. FDA defines end of support as the point beyond which the manufacturer ceases to provide support (www.fda.gov), so component end-of-support dates should be reviewed at every release.

Performance and Benchmarks: What the Evidence Shows About SBOM Quality

Published measurements describe open-source repositories rather than medical-device firmware, so they indicate direction, not device-specific performance. A 2026 preprint evaluating 55,444 SBOMs from six tools across 3,287 repositories (arxiv.org) reported inter-tool consistency for package detection as low as 7.84% to 12.77% (arxiv.org). A study of 2,414 repositories (arxiv.org) reported the scanner false-positive finding above.

Two design conclusions follow. A single generator's output should not be treated as ground truth, so an independent cross-check, such as a binary scan of the final image, should reconcile against the build-time SBOM. And identifier-based vulnerability matching produces candidates that need device-specific assessment. No public benchmark measures SBOM accuracy specifically for medical-device firmware.

Data Analysis and Evidence

Adoption and barrier statistics

The Linux Foundation's 2022 research surveyed 412 organizations with a 65-question instrument (www.linuxfoundation.org); 47% were producing or consuming SBOMs (www.linuxfoundation.org) and 78% expected to do so in 2022 (www.linuxfoundation.org). ENISA's 2026 survey found 78% had initiated SBOM adoption (www.enisa.europa.eu). The surveys differ in date, geography and sampling and should not be read as a trend line.

Vulnerability data volume is growing: as of November 2026, CVE.org's metrics page reported about 29,000 published Common Vulnerabilities and Exposures (CVE) records for 2023 (www.cve.org) and about 48,000 for 2025 (www.cve.org), an increase of about 67% computed from the two figures (exact counts vary slightly with snapshot date and counting basis).

Proposed SBOM completeness metrics

These formulas are analyst constructs for use as pipeline gates. The thresholds are examples each manufacturer should set and justify; none is an FDA requirement.

- **Identification coverage** = identified components in the SBOM / components discovered by an independent scan of the release artifact. Example gate: 95% or higher, with every gap listed.
- **Version completeness** = components with a version / components in the SBOM. Example gate: 100% for third-party components.
- **Hash completeness** = components with a hash / components in the SBOM. N73 recommends hashes and the 2026 CISA elements add them (content.govdelivery.com).
- **Unresolved supplier components** = components with unknown supplier or producer / components in the SBOM. Example gate: zero without a documented justification.

- **Support-data completeness** = components with a support level and end-of-support entry / components in the SBOM, derived from FDA's two additional attributes.
- **Stale-SBOM age** = days between the SBOM timestamp and the evaluation date. Example gate: regenerate at every release and re-triage on a defined cycle.

Case Studies and Real-World Examples

Synthetic Infusion Gateway Firmware (Hypothetical Example)

This example is entirely synthetic. "Example Medical Devices Inc.," the gateway firmware and every component, number and date are invented, and no real product, supplier or secret is represented. The JSON below was hand-written for this report and was not run through a schema validator or conformance tool; teams should validate any adopted example with the tools above and should not infer that it demonstrates compliance.

Scenario. Gateway firmware 3.2.1 is built on October 2, 2026. A post-build scan discovers 412 components, and the build-time SBOM identifies 398.

Metric	Calculation	Result
Identification coverage	398 / 412	96.6%
Version completeness	392 / 398	98.5%
Hash completeness	380 / 398	95.5%
Unresolved supplier components	9 / 398	2.3%
Stale-SBOM age on November 11, 2026	October 2 to November 11	40 days

Against example gates of 95% identification, 100% version completeness and zero unresolved suppliers, the build would fail on version completeness (6 components without a version) and on 9 unresolved suppliers. The team would fix them or document each justification before the eSTAR handoff.

CycloneDX 1.7 sketch (abridged).

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.7",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "metadata": {
    "timestamp": "2026-10-02T14:05:00Z",
    "lifecycles": [{ "phase": "post-build" }],
    "authors": [{ "name": "Example Product Security Team" }],
    "component": {
      "type": "firmware", "bom-ref": "fw-gateway", "name": "example-gateway-fw", "version": "3.2.1",
      "manufacturer": { "name": "Example Medical Devices Inc." }
    }
```

```
  },
  "components": [{
    "type": "library", "bom-ref": "lib-examplelib", "name": "examplelib", "version": "1.4.2",
    "supplier": { "name": "Example Library Project" },
    "purl": "pkg:generic/examplelib@1.4.2",
    "hashes": [{ "alg": "SHA-256", "content":
"a1b2c3d4e5f60718293a4b5c6d7e8f90a1b2c3d4e5f60718293a4b5c6d7e8f90" }],
    "licenses": [{ "license": { "id": "MIT" } }],
    "properties": [
      { "name": "example:support-level", "value": "actively-maintained" },
      { "name": "cdx:lifecycle:milestone:endOfSupport", "value": "2028-06-30" }
    ]
  }],
  "dependencies": [
    { "ref": "fw-gateway", "dependsOn": ["lib-examplelib"] },
    { "ref": "lib-examplelib", "dependsOn": [] }
  ],
  "compositions": [{ "aggregate": "incomplete", "assemblies": ["fw-gateway"] }]
}
```

SPDX 2.3 sketch (abridged).

```
{
  "spdxVersion": "SPDX-2.3",
  "dataLicense": "CC0-1.0",
  "SPDXID": "SPDXRef-DOCUMENT",
  "name": "example-gateway-fw-3.2.1-sbom",
  "documentNamespace": "https://sbom.example.com/spdx/example-gateway-fw/3.2.1/0001",
  "creationInfo": {
    "created": "2026-10-02T14:05:00Z",
    "creators": ["Tool: example-sbom-generator-1.0.0", "Organization: Example Medical Devices Inc."],
    "comment": "Generation context: post-build"
  },
  "packages": [
    { "SPDXID": "SPDXRef-Firmware", "name": "example-gateway-fw", "versionInfo": "3.2.1",
      "supplier": "Organization: Example Medical Devices Inc.", "downloadLocation": "NOASSERTION",
      "filesAnalyzed": false, "primaryPackagePurpose": "FIRMWARE" },
    { "SPDXID": "SPDXRef-examplelib", "name": "examplelib", "versionInfo": "1.4.2",
      "supplier": "Organization: Example Library Project", "downloadLocation": "NOASSERTION",
      "filesAnalyzed": false, "primaryPackagePurpose": "LIBRARY",
      "checksums": [{ "algorithm": "SHA256", "checksumValue":
"a1b2c3d4e5f60718293a4b5c6d7e8f90a1b2c3d4e5f60718293a4b5c6d7e8f90" }],
      "licenseConcluded": "MIT", "licenseDeclared": "MIT", "validUntilDate": "2028-06-30T00:00:00Z",
      "externalRefs": [{ "referenceCategory": "PACKAGE-MANAGER", "referenceType": "purl",
"referenceLocator": "pkg:generic/examplelib@1.4.2" }] }
  ],
  "relationships": [
    { "spdxElementId": "SPDXRef-DOCUMENT", "relationshipType": "DESCRIBES", "relatedSpdxElement": "SPDXRef-
Firmware" },
    { "spdxElementId": "SPDXRef-Firmware", "relationshipType": "DEPENDS_ON", "relatedSpdxElement": "SPDXRef-
examplelib" }
```

```
  ]
}
```

Validation tests to automate before the eSTAR handoff:

- **Schema test:** validate against the schema for the declared version, using the CycloneDX validator or the SPDX Python tools.
- **Round-trip test:** convert to the second format and diff name, version, supplier, hash and relationship counts. The CycloneDX command-line tool converts among CycloneDX serializations and SPDX JSON 2.3; record any field loss.
- **Minimum-element test:** run the conformance checker for NTIA and CISA elements (github.com).
- **Extension test:** assert that support-level and end-of-support properties exist for every third-party component.
- **Join test:** confirm the SBOM resolves to a device version and unique device identifier.

Implications and Future Directions

Format convergence is incomplete but narrowing. CISA's 2026 elements emphasize machine-processable formats (content.govdelivery.com), and the multinational Shared Vision guidance says an SBOM should be machine-processable in a widely used format (www.cisa.gov) while warning that divergent implementations could hinder adoption (www.cisa.gov). CISA's earlier sharing report found that no single sharing solution had become ubiquitous (www.cisa.gov), so manufacturers should expect to publish in more than one format.

Specification churn. CycloneDX 1.7 is current, SPDX 3.0.1 is the latest SPDX edition, and SPDX 3.1 had not reached general availability as of November 2026. Pin the specification version in the SBOM profile, test upgrades on a branch, and record the version in the design history file, since tools may support only some versions.

Quality-system alignment. FDA describes a Secure Product Development Framework (SPDF) as one approach to help ensure the QMSR is met (www.fda.gov); embedding SBOM gates there, with supplier contract terms for per-release SBOMs (healthsectorcouncil.org), gives reviewers one process to examine.

Regulatory questions. None of the cited sources prescribes a format, so device-specific regulatory questions belong with qualified regulatory counsel and FDA's Q-Submission process.

Frequently Asked Questions (FAQs)

Does FDA require CycloneDX or SPDX?

None of the cited sources names either format as required. The statute requires an SBOM for cyber devices, the guidance recommends NTIA-consistent, machine-readable SBOMs (www.fda.gov), and IMDRF N73 lists both formats without ranking them (www.imdrf.org).

What are the FDA SBOM requirements for medical devices?

For cyber devices, provide an SBOM covering commercial, open-source and off-the-shelf components. The guidance recommends the Section V.A.4.b content: NTIA-consistent fields plus support level and end-of-support date.

Which SBOM format should be used in a premarket submission?

Choose one canonical format, document the rationale and validate it. Yocto programs may favor SPDX; programs wanting integrated vulnerability analysis may favor CycloneDX (cyclonedx.org).

How does section 524B relate to the cybersecurity guidance?

Section 524B is the statute governing postmarket plans, patching and the SBOM (www.law.cornell.edu). The guidance contains FDA's recommendations on meeting and documenting them.

What happens if the eSTAR cybersecurity section is incomplete?

FDA says the eSTAR will be put on a Technical Screening hold.

What are the NTIA minimum elements, and are they current?

NTIA's 2021 document defines seven data fields (www.ntia.doc.gov). CISA's July 2026 Minimum Elements update and replace them (www.cisa.gov), while FDA's guidance still refers to NTIA baseline attributes.

What SBOM best practices apply, and how are SBOMs managed after release?

Generate in the build, merge supplier SBOMs with provenance, validate, sign, archive, and refresh with each release. Trace the SBOM to the risk file, monitor third-party components for new vulnerabilities, and plan for end of support.

What is VEX, and is it required?

VEX is a machine-readable statement of a vulnerability's status for a product (www.cisa.gov). The guidance text reviewed did not mention it, and FDA states VEX alone does not replace the vulnerability assessment.

Conclusion

The February 2026 FDA guidance and section 524B together make an SBOM a statutory element of a cyber-device submission while leaving format choice to the manufacturer. The decisive work lies in the surrounding system: a documented SBOM profile covering the NTIA and CISA fields and FDA's two support attributes, a build pipeline that generates and validates SBOMs, supplier terms that deliver machine-readable inputs, a vulnerability and VEX workflow that supports the risk assessment, and change control that issues a new SBOM whenever the software changes.

CycloneDX and SPDX can both carry the core fields. CycloneDX offers integrated vulnerability analysis and signing options, and SPDX offers an ISO-lineage edition, strong embedded-build support and native end-of-support fields. The evidence on tool disagreement and completeness barriers argues for measurement and

cross-checking over reliance on any single generator. Teams should verify current guidance, the eSTAR template and specification versions at the time of submission, and consult regulatory counsel and FDA for device-specific questions.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.law.cornell.edu/uscode/text/21/360n-2
2. https://www.fda.gov/media/119933/download
3. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs
4. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
5. https://www.imdrf.org/sites/default/files/2023-04/Principles%20and%20Practices%20for%20Software%20Bill%20of%20Materials%20for%20Medical%20Device%20Cybersecurity%20%28N73%29.pdf
6. https://www.cisa.gov/sites/default/files/2026-07/2026_cisa_sbom_minimum_elements_508c.pdf
7. https://ecma-international.org/publications-and-standards/standards/ecma-424
8. https://cyclonedx.org/docs
9. https://spdx.github.io/spdx-spec/v2.3/package-information
10. https://spdx.github.io/spdx-spec/v3.0.1/model/Security/Classes/VexNotAffectedVulnAssessmentRelationship
11. https://arxiv.org/abs/2601.05622
12. https://www.enisa.europa.eu/sites/default/files/2026-06/SBOM%20Adoption%20State%20of%20Play%202026.pdf
13. https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity
14. https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
15. https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom
16. https://www.cisa.gov/resources-tools/resources/2026-minimum-elements-software-bill-materials-sbom
17. https://content.govdelivery.com/accounts/USDHSCISA/bulletins/422a7eb
18. https://owasp.org/www-project-cyclonedx
19. https://cyclonedx.org/news/cyclonedx-v1.7-released
20. https://cyclonedx.org/specification/overview
21. https://cyclonedx.org/tool-center
22. https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-SBOM-en.pdf
23. https://github.com/CycloneDX/specification
24. https://arxiv.org/abs/2512.21781
25. https://cyclonedx.org/capabilities/bomlink
26. https://cyclonedx.github.io/cyclonedx-property-taxonomy/cdx/lifecycle.html
27. https://spdx.dev/about/overview
28. https://spdx.dev

29. https://spdx.github.io/spdx-spec/v2.3/conformance
30. https://github.com/spdx/spdx-spec/releases
31. https://spdx.github.io/spdx-spec/v3.0.1/serializations
32. https://spdx.github.io/spdx-spec/v3.0.1/conformance
33. https://spdx.github.io/spdx-spec/v3.0.1/model/Core/Properties/validUntilTime
34. https://spdx.github.io/spdx-spec/v3.0.1/model/Core/Vocabularies/SupportType
35. https://spdx.github.io/spdx-spec/v3.0.1/model/Software/Vocabularies/SoftwarePurpose
36. https://docs.yoctoproject.org/dev/dev-manual/sbom.html
37. https://docs.zephyrproject.org/latest/develop/west/zephyr-cmds.html
38. https://github.com/microsoft/sbom-tool
39. https://spdx.github.io/spdx-spec/v2.3/relationships-between-SPDX-elements
40. https://spdx.github.io/spdx-spec/v2.3/regulations-compliance
41. https://spdx.github.io/spdx-spec/v3.0.1/model/Core/Vocabularies/RelationshipCompleteness
42. https://spdx.github.io/spdx-spec/v3.0.1/model/Software/Vocabularies/SbomType
43. https://github.com/Microsoft/sbom-tool/blob/main/docs/sbom-tool-arguments.md
44. https://github.com/spdx/ntia-conformance-checker
45. https://github.com/CycloneDX/cdxgen
46. https://github.com/CycloneDX/cyclonedx-cli
47. https://spdx.github.io/spdx-spec/v2.3/document-creation-information
48. https://spdx.github.io/spdx-spec/v3.0.1/model/Software/Properties/packageUrl
49. https://spdx.github.io/spdx-spec/v3.0.1/model/Security/Classes/ExploitCatalogVulnAssessmentRelationship
50. https://healthsectorcouncil.org/wp-content/uploads/2024/03/Medical-Technology-and-Health-IT-Joint-Security-Plan-v2.pdf
51. https://trivy.dev/latest/docs/supply-chain/sbom
52. https://github.com/spdx/tools-python
53. https://github.com/anchore/syft
54. https://docs.sigstore.dev/cosign/verifying/attestation
55. https://docs.sigstore.dev/cosign/signing/other_types
56. https://slsa.dev/attestation-model
57. https://www.fda.gov/media/152429/download
58. https://www.fda.gov/medical-devices/how-study-and-market-your-device/estar-program
59. https://www.cisa.gov/sites/default/files/2023-04/minimum-requirements-for-vex-508c.pdf
60. https://github.com/openvex/spec/blob/main/OPENVEX-SPEC.md
61. https://docs.oasis-open.org/csaf/csaf/v2.1/csaf-v2.1.html
62. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
63. https://www.first.org/epss
64. https://www.first.org/epss/how-it-works.html
65. https://arxiv.org/abs/2511.20313

66. https://www.cisa.gov/sites/default/files/2023-01/VEX_Status_Justification_Jun22.pdf
67. https://www.fda.gov/media/95862/download
68. https://health-isac.org/leveraging-sboms-to-strengthen-cyber-resilience
69. https://docs.dependencytrack.org
70. https://dependencytrack.github.io/docs
71. https://www.linuxfoundation.org/press/press-release/the-linux-foundation-releases-the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness-research
72. https://www.cve.org/About/Metrics
73. https://www.cisa.gov/sites/default/files/2025-09/joint-guidance-a-shared-vision-of-software-bill-of-materials-for-cybersecurity_508c.pdf
74. https://www.cisa.gov/sites/default/files/2023-04/sbom-sharing-lifecycle-report_508.pdf

THE PUBLISHER

About IntuitionLabs

IntuitionLabs is an AI consulting, custom software development and data engineering firm serving pharmaceutical, biotechnology, medical-device and other life-science organizations. We work with clinical, regulatory, medical-affairs, commercial, quality and IT teams to connect technology decisions with the work people need to accomplish.

AI consulting and adoption

Our AI enablement services cover readiness assessments, use-case selection, governance and policies, team workshops, adoption measurement and ongoing advisory support. We help organizations structure the information layer behind AI: source material, context, permissions and maintained knowledge that make generated answers useful and reviewable. Private LLM inference and hosted AI options support teams evaluating how to operate AI with appropriate control over their data and infrastructure.

Software, data and life-science workflows

IntuitionLabs develops custom software for pharma and biotech, integrates enterprise systems, and builds data engineering and business intelligence solutions. Areas of focus include AI agents, regulatory research, medical writing, medical affairs, CMC information, competitive intelligence and clinical-document workflows. Our eTMF intelligence work includes cross-system reconciliation and inspection-readiness support.

Enterprise platforms and regulated delivery

We provide Veeva services, application support, managed services, integrations and custom applications, alongside enterprise content work involving platforms such as Egnyte. For regulated workflows, our services include GxP enablement, computer-system validation and software development addressing 21 CFR Part 11 requirements. The applicable controls, validation responsibilities and acceptance criteria are defined for each engagement.

Work with IntuitionLabs

Explore AI enablement, pharma and biotech software development, data engineering and BI, and Veeva services. Contact IntuitionLabs to discuss your workflow, information sources and implementation needs.

IntuitionLabs publishes educational research to help life-science teams make informed technology decisions. Coverage of a product or organization does not imply a client relationship, endorsement or partnership.

Website: https://intuitionlabs.ai

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.