Strike Graph

FDA Medical Device SBOM Compliance Checklist

❑ **Determine if your device needs an SBOM**

Does your device qualify as a cyber device? That means:

- It includes software.
- It connects to the internet.
- It contains technological characteristics that are vulnerable to cybersecurity threats.

◊ If yes, you must submit an SBOM with your FDA premarket application.

◊ If no, an SBOM isn't required but is still recommended as a best practice.

❑ **Include the 7 NTIA baseline attributes (required for all components):**

- ❑ Author name
- ❑ Timestamp (ISO 8601 format preferred)
- ❑ Supplier name
- ❑ Component name
- ❑ Version string
- ❑ Unique identifier
- ❑ Dependency relationship (how components relate to each other)

❑ **Cover the full software inventory**

- ❑ Include all manufacturer-developed, third-party, and open-source software.
- ❑ Include any nested or dependent components your software relies on.
- ❑ Use a machine-readable format (e.g., CycloneDX, SPDX, or SWID) unless a spreadsheet is more practical for simple SBOMs.

❑ **Include additional component-level details**

- ❑ Level of support – is the software still actively maintained?
- ❑ End-of-support date – when will updates or patches stop?

❑ **Include known vulnerabilities**

- ❑ Check each component against databases like the CISA KEV Catalog.
- ❑ Include vulnerability information in the SBOM or as a separate addendum.
- ❑ Use VeX statements when appropriate to explain why a vulnerability may not apply.

For each vulnerability:

- ❑ Explain how it was found (e.g., scanning tools, manual review).
- ❑ Assess the risk to device function and patient safety.
- ❑ Describe your response, including any compensating controls if a patch isn't possible.

❑ **Post-market responsibilities**

- ❑ Monitor your SBOM over time for new vulnerabilities.
- ❑ Update the SBOM as the software changes.
- ❑ Notify customers of changes or emerging threats.
- ❑ Include response timelines and metrics in your annual report to the FDA.