

SBOM checklist for device makers

For each firmware release you ship. Formats: CycloneDX (ECMA-424) or SPDX (ISO/IEC 5962:2021).

- ☐ Produce an SBOM for every firmware release you ship, not once a year.
- ☐ Use CycloneDX or SPDX, in a machine-readable form.
- ☐ Record for each component its supplier, name, version, a unique identifier such as a PURL or CPE, and its dependencies, plus the SBOM's author and timestamp.
- ☐ Cover at least the top-level dependencies, and include the chip vendor's SDK, the kernel, BusyBox and the C and TLS libraries.
- ☐ Include the binaries you did not build from source, identified from the image.
- ☐ Record the firmware version and hash each SBOM describes.
- ☐ Match the components to known vulnerabilities and record which apply, with VEX.
- ☐ Keep the SBOM of every shipped release, and for the EU with the technical documentation.
- ☐ Decide who receives SBOMs, such as buyers, labs or authorities, and how.

Sources

- NTIA, The Minimum Elements For a Software Bill of Materials (SBOM): <https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom>
- Regulation (EU) 2024/2847, the Cyber Resilience Act, Annex I, Part II: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>

A guide to where the evidence is, not legal advice or certification. Your lab, notified body or regulator makes the final call.
magdox.io/blog/sbom-for-device-makers/