Stonetusker Insights · Technical note on DevSecOps and software supply chain

# The 2026 Minimum Elements for a Software Bill of Materials: Check Your Latest Release Record in 30 Minutes

On 29 July 2026 the Cybersecurity and Infrastructure Security Agency published a new baseline for what a software bill of materials should contain. It adds hashes, licences, the tool name, the generation context and a signature. One query on your latest release record shows how far you are from it.

**For:** Teams that sell software or devices to United States government, regulated or large enterprise buyers.
**Skip if:** Nobody asks you for a software bill of materials yet.

By Subeesh Sivanandan, Founder, Stonetusker Systems · Updated 29 October 2026 · About 3 minutes to read · PDF version

Technical and engineering guidance. Please confirm legal obligations with your own counsel.

## The short version

- On 29 July 2026 the Cybersecurity and Infrastructure Security Agency published the 2026 Minimum Elements for a Software Bill of Materials. It updates the 2021 baseline.[1,2]
- New elements include the component hash, the component licence, the tool name and the generation context, plus a field for the author signature.[1,3]
- Generation context shows whether a record came from inside the build or from a scan afterwards. Careful buyers notice the difference.
- One query on your latest release record shows the share of components with a hash, a licence and a package URL.

**29 July 2026**
Final guidance published[1]

**4**
New data fields the agency names: hash, licence, tool name and generation context[1]

**2021**
Year of the earlier baseline that the new guidance updates[2]

## Why it matters now

For five years the reference list was the 2021 set of minimum elements from the National Telecommunications and Information Administration. The 2026 guidance updates it.[1,2] It adds the component hash, the component licence, the tool name and the generation context. It also adds a field for a digital signature from the author of the record, so a customer can check that the record is genuine.[3,4]

Generation context matters most in practice. The official text accepts references such as "before build", "build" and "after build".[4] A record produced during the build describes what was built. A scan afterwards infers what is inside and can miss code that was statically linked or vendored.

The guidance itself is voluntary. Federal buyers and many enterprise customers in the United States use it as their baseline. Medical device makers have had to provide a software bill of materials to the Food and Drug Administration since March 2023,[6] and the main obligations of the European Union Cyber Resilience Act apply from 11 December 2027.[7]

# Check your latest release record in 30 minutes

## Step 1. Measure a CycloneDX record

Take the record for your most recent production release.

```
jq '{
  tools: [(.metadata.tools.components? // .metadata.tools // [])[] |
.name],
  lifecycle: .metadata.lifecycles,
  signed: has("signature"),
  components: (.components // [] | length),
  with_hash: ([.components[]? | select((.hashes // []) | length >
0)] | length),
  with_license: ([.components[]? | select((.licenses // []) | length
> 0)] | length),
  with_purl: ([.components[]? | select(.purl)] | length)
}' sbom.cdx.json
```

Since CycloneDX 1.5 the tool sits under `metadata.tools.components`. The older list form of `metadata.tools` is marked deprecated.[5] The query reads both forms. `signed` only detects an embedded signature, so check for a detached signature or attestation next to the release as well.

### Step 2. Or measure an SPDX 2.3 record

```
jq '{
  creators: .creationInfo.creators,
  packages: (.packages // [] | length),
  with_checksum: ([.packages[]? | select((.checksums // []) | length
> 0)] | length),
  with_license: ([.packages[]? | select((.licenseConcluded //
"NOASSERTION") != "NOASSERTION" or (.licenseDeclared //
"NOASSERTION") != "NOASSERTION")] | length)
}' sbom.spdx.json
```

### Step 3. Compare the ratios

Divide each count by the number of components. Then confirm two points: the record states its generation context, and it carries a signature.

## What the result means

| What you find | What it means | Typical effort |
|---|---|---|
| Hash, licence and package URL above about 90%, a build lifecycle and a signature | The record is close to the 2026 elements | Spot fixes for the remaining components |
| Ratios below about 90% | A gap that a careful customer will notice | Generator settings and a review of unknown entries |
| No lifecycle, or a record made by a separate scan job | The record is an inference, not a build record | Move generation into the build; usually a few weeks |

| What you find | What it means | Typical effort |
|---|---|---|
| No signature | A customer cannot confirm the record is unaltered | Add signing to the release job |

# The move, step by step

1. **Generate in the build job.** Produce the record in the same pipeline run that builds the release, with build-aware tools such as Yocto create-spdx, CycloneDX build plugins, cdxgen or Syft on the build output.
2. **Add hashes and identifiers.** Record a cryptographic hash and a package URL for every component, and fix the components that come out without them.
3. **Record tool and context.** Write the tool name, its version and the lifecycle phase into the record metadata.
4. **Add licences.** Fill declared licences from package metadata and review the unknown entries.
5. **Sign and store.** Sign the record, for example as a Sigstore cosign attestation or a detached signature next to a firmware file, and store it with the release artifact.

Keep your existing format. SPDX and CycloneDX can both carry the new elements. What usually changes is when the record is produced and which fields your tools fill in.

# What is still open

- Tool support for the new fields is still maturing, especially for signatures and lifecycle information.
- The guidance notes that some software types, such as artificial intelligence and software as a service in cloud environments, may require additional elements.[1,3]
- The European Commission may specify its own format and elements for the record under the Cyber Resilience Act.

# A note to forward to your team

Software bill of materials check against the 2026 minimum elements

The Cybersecurity and Infrastructure Security Agency published new minimum elements for a software bill of materials on 29 July 2026. They add hashes, licences, tool name, generation context and a signature.

Please run the query in this note on the record for [product and release] by [date] and reply with:
1. Components in the record
2. Components with a hash
3. Components with a licence
4. Generation context stated: [yes or no]
5. Record signed: [yes or no]

Owner: [name]
Note: https://stonetusker.com/insights/cisa-sbom-minimum-elements-2026.html

# Questions

### What are the 2026 minimum elements?

Final guidance from the Cybersecurity and Infrastructure Security Agency, published on 29 July 2026, that updates the 2021 minimum elements. It adds component hash, licence, tool name, generation context and an author signature, and renames several fields.

### Do we need a new format?

SPDX and CycloneDX can both carry the new elements. The usual change is when the record is produced and which fields the tools fill in.

### What is generation context?

It records the lifecycle phase in which the record was produced, such as before, during or after the build. Build records describe what was built; records made after the build are inferred by scanning.

### Is the guidance mandatory?

The guidance itself is voluntary. Federal buyers, regulated industries and many enterprise customers in the United States use it as the baseline for supplier expectations.

## Want a second opinion?

Run the check yourself first. If you would like a second opinion, reply with three counts only: the components in your latest record, how many have a hash and how many have a licence. No product names, files or tool output are needed. Within five working days you receive a short written review with the likely gaps against the 2026 elements, the pipeline changes that close them and a time estimate. It is free and confidential, and a call is optional.

**Ask for a second opinion**

The button opens an email to subeesh@stonetusker.com with the subject and the numbers to fill in. You can also use the contact page, or reply to the email or LinkedIn message that brought you here.

# Next page for your situation

- Cyber Resilience Act and Yocto Kirkstone: the European Union reporting duty that depends on the same record.
- Bitnami images: frozen images that show up in the record.

## Sources


1. CISA: United States Government and international partners release updated minimum elements for a software bill of materials (29 July 2026)
2. Help Net Security: CISA sets a new SBOM baseline (July 2026)
3. Industrial Cyber: CISA refreshes SBOM guidance with new data fields
4. Australian Cyber Security Centre (co-author): 2026 Minimum Elements for a Software Bill of Materials
5. CycloneDX: version 1.5 JSON reference
6. Food and Drug Administration: Cybersecurity in medical devices, frequently asked questions
7. European Commission, Interoperable Europe: Cyber Resilience Act now effective


## About the author


Subeesh Sivanandan is the Founder and CEO of Stonetusker Systems. He has worked for more than 27 years in release engineering, DevOps, platform engineering & embedded Linux. His career includes serving as the Principal Engineer & Manager of Release Engineering at Stryker, alongside earlier roles at Nokia, VeriSign, and IP Infusion. LinkedIn profile.


## Revision history (recent 3 updates)

Version 2.1, 29 October 2026. Every fact on this page is checked against a minimum of two sources each month.

| Version | Date | Change |
|---|---|---|
| 1.4 | 16 October 2026 | Rewritten as an article for quick readers: introduction, summary of all major changes, what it means and first steps; one figure; commands folded for platform leads; print option and direct email offer |
| 2.0 | 25 October 2026 | Simpler layout and shorter text; the review offer now asks for a few counts only |

| Version | Date | Change |
|---|---|---|
| 2.1 | 29 October 2026 | Who-this-is-for box, email offer with the numbers listed, and next pages |