SBOM in the Age of Global Regulation

Everyone seems to care about SBOMs now (yay?)

Christopher “CRob” Robinson
Chief Technology Officer/Chief Security Architect - OpenSSF/Linux Foundation

SBOMit! Workshop
November 11, 2025

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Who is this guy?

CRob, n, adj, and v

Pronunciation: U.S. (K-rowb)

chmod 666 crob.md

44th level Dungeon Master

27th level Securityologist

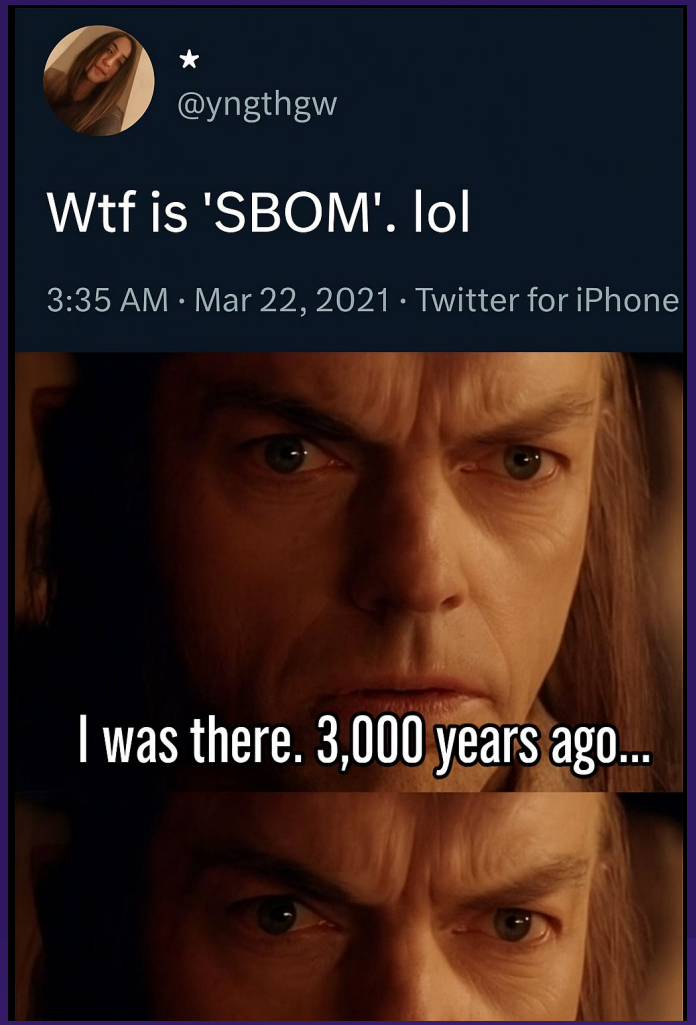
Pirate-enthusiast & hat-owner

Chief Technology Officer & Chief Security Architect, OpenSSF - Linux Foundation

Involved in upstream OSS CVD for ~15 years

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Most images generated by ChatGPT, except that -> That's just my pal Gimp!



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Image Source

Brief SBOM tangent……

https://www.youtube.com/watch?v=sNjVQaK5QW4

Cyberface says *"Say 'SBOM' three times and Alan will appear!"*

What are SBOMs?

- This is a machine-readable artifact that collects all of the components and dependencies included within a piece of software or product.
- SBOMs should enable orgs to quickly see a list of components and versions included within software and be able to compare that to known CVE lists to understand what actions may need to be taken after a vuln report

Why SBOMs? Why NOW?

Supply-chain risk is mainstream; buyers and regulators demand software transparency

SBOM = inventory + context → faster triage, fewer fire drills

Goal: align global rules with practical, automatable workflows

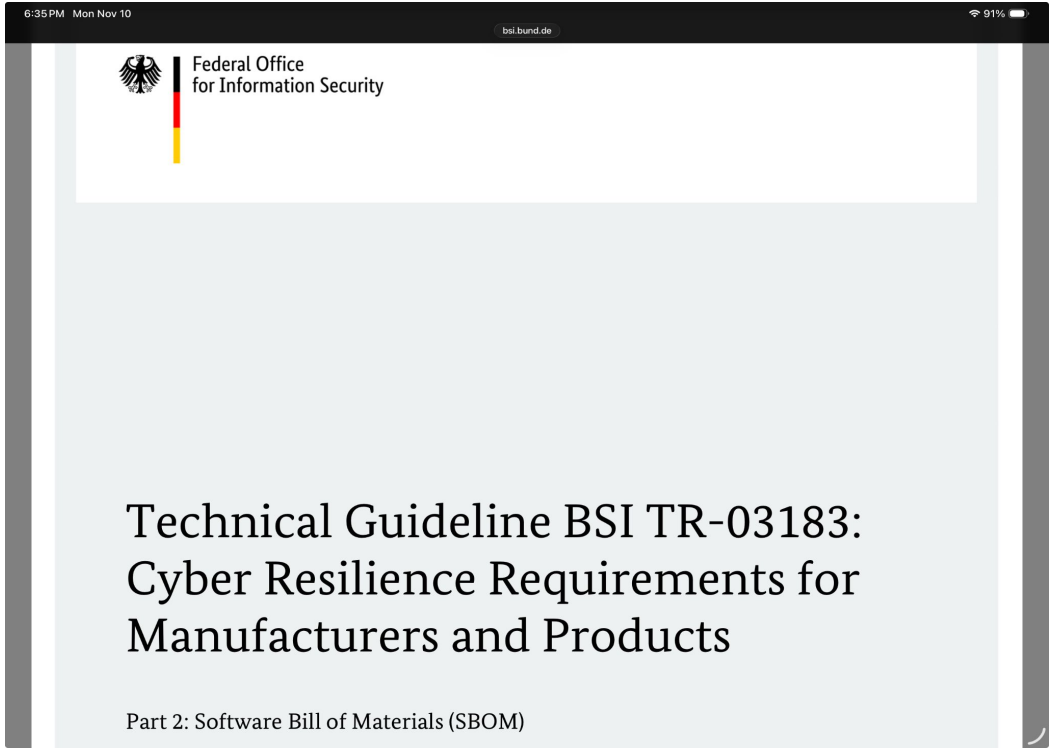
30,000ft view of SBOM-adjacent Regulations

- **US WH Executive Order 14028 — "Improving the Nation's Cybersecurity"**: (May 2021) Directs NIST & NTIA to create minimum elements for SBOMs
- **US WH Executive Order 14110 — "Safe, Secure, and Trustworthy Artificial Intelligence"** - (Oct 2023) reinforces that SBOM-like transparency measures should extend to AI software supply chains
- Japan's METI **"Guide of Introduction of Software Bill of Materials (SBOM) for Software Management" Ver. 1.0** Published July 2023 and updated August 2024
- **EU Cyber Resilience Act (CRA)**: lifecycle security + incident/vuln reporting; SBOM expectations emerging in guidance and harmonized standards. Enters into force Dec 30, 2024; vuln-reporting to ENISA/CSIRTs by **Sep 11, 2026**; broader enforcement by **Dec 2027**.
- **A Shared Vision of SBOM for Cybersecurity - Sept 3, 2025 -** 17 international organizations issuing a joint paper on SBOMs
- **U.S. Federal**: CISA updated **SBOM Minimum Elements (2025)**; evolving maturity framing.
- **U.S. FDA (medical devices)**: Final premarket cybersecurity guidance (June 2025) expects SBOM as part of submissions.

Standards you can ship today

- **SPDX**: ISO/IEC 5962:2021; v3.0/3.0.1 extends profiles (security, AI, build).
- **CycloneDX**: 1.6 (CBOM, attestations) and **1.7 (Oct 2025)**; recognized as an **ECMA** standard.
- **CSAF** (for advisories) now also an ISO/IEC standard; VEX profile communicates exploitability.
- **NTIA** - OG SBOM materials
- **CISA** - Next Generation of SBOM collab (Old and revised Minimum Elements)
- **ENISA** - EU's designation cyber coordinator for the National CSIRTs
- **BSI** - Germany's National CSIRT leading the union in practical implementation guidance
- **ETSI + CEN/CENELEC** - EU standards bodies developing new CRA-related standards for SBOMs

BSI Technical Guide for SBOMs



National CERTs in the EU, like the German BSI, are all composing guidance for their citizens and resident manufacturers on what they would like to see from SBOMs

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2_v2_1_0.pdf?__blob=publicationFile&v=5

CISA’s 2025 SBOM Minimum Elements (what’s new)

Lifecycle obligations + reporting to ENISA/CSIRTs (24h for actively exploited vulns) push orgs to know “what’s in the box” and exposure quickly.

Expect harmonized standards to reference SBOM content/quality; plan for attestations and provenance.

Data Fields

- SBOM Author (Major Update)
- Software Producer (Major Update)
- Component Name (Major Update)
- Component Version (Major Update)
- Software Identifiers ((Major Update)
- Component Hash (New)
- License (New)
- Dependency Relationship (Major Update)
- Tool Name (New)
- Timestamp (Minor Update)
- Generation Context (New)

Automation Support

- CycloneDX or SPDX

Practices & Processes

- Frequency (Minor Update)
- Coverage (Major Update)
- Known Unknowns (Major Update)
- Distribution & Delivery (Minor Update)
- Accomodation of Update to SBOM Data (Major Update)

From inventory to action: SBOM + VEX + advisories

VEX answers: “Is *this* vuln exploitable in *this* product/version?” (less noise)

CSAF = machine-readable advisories; vendors (e.g., Red Hat) publish CSAF and VEX.

OpenVEX exists as a lightweight, embeddable approach; growing ecosystem.

Notes: The story: SBOM reduces search space; VEX/CSAF prioritizes reality.

Interop: choosing a format (and why it shouldn’t hurt)

If your toolchain is license+security heavy → SPDX 3 profiles help. FOSSA

If you want rich supply-chain/ops artifacts → CycloneDX 1.6/1.7 (CBOM, attestations). CycloneDX+1

Convertors exist; focus on content quality and automation, not bikeshedding.

Notes: Encourage one primary format internally + gateway conversion as needed.

The Need for SBOM Accuracy & Completeness

- Laws like the CRA REQUIRE Manufacturers to create accurate and complete SBOMs.
- These laws typically do NOT put obligations on upstream developers.
- With these obligations, it is expected that downstream starts asking/demanding/begging for more data to be provided upstream to make their compliance easier.
- Downstream consumers often have to aggregate dozens to hundreds of artifacts like SBOMs to fully understand the software in their organizations.

CRA Enters the Chat

- **Penalties** - between 1%-2.5% of your global revenue for EACH infraction penalties for bad docs/sboms!!
- **Provide the Commission and other Authorities false or misleading data** (like incomplete SBOMs) that's a 1% penalty for EACH infraction How many dependencies DO you have?
- **Timelines,timelines, timelines!** - 24hrs to report vulnerabilities that are being actively exploited to the EU authorities. 72 hrs to have an advisory published with details, workarounds and strongly encouraged fix

What “good” SBOM practice looks like in 2025

Completeness & depth (transitive deps, hashes, licenses, and build meta)

Freshness (per-build or per-release SBOMs; not once-a-year PDFs)

Provable provenance (signing/attestations; tie to CI)

Context (link to advisories + VEX)

Pipeline pattern

CI step generates SBOM → sign → store (artifact repo)

Nightly vuln sync → map advisories (CSAF) → generate/ingest VEX

Exposure dashboard per product/version; evidence export for CRA/FDA/CISA asks

Notes: Stress “evidence at your fingertips” when a regulator or customer knocks.

Common pitfalls to avoid

Static, manual SBOMs (quickly stale)

No package identity normalization (matching breaks)

Missing build/provenance data (can’t trust/integrate)

VEX silence (forces teams to chase non-issues)

Notes: If you can only fix one: automate generation in CI and sign outputs.

Buyer ↔ supplier contract basics

Require **machine-readable** SBOM (SPDX or CycloneDX) per release, with signatures

Require mapping to **CSAF** advisories and VEX for exploitable status

Set SLAs for **update cadence** and vulnerability status changes

Notes: Keep it vendor-neutral; focus on outcomes and formats, not tools.

What to watch in 2025–2027

CRA implementation guides & harmonized standards touching SBOM quality/provenance. EU CRA Digital Strategy

CISA's evolving **Minimum Elements** and tooling guidance. CISA

Rapid spec iteration (SPDX 3 profiles; CycloneDX 1.7+; CSAF in more vendors).

Notes: Keep an eye on convergence: fewer arguments, more automation.

Key Takeaways

Regulation is converging on **actionable** SBOMs, not just lists

Use **SPDX/CycloneDX + CSAF/VEX** to reduce noise and prove diligence

Automate in CI, sign everything, and ship context with every release

Notes: End with “your next step” ask.

Key Dates + Key Docs

- CRA: entered into force **Dec 30, 2024**; vuln reporting by **Sep 11, 2026**; broad enforcement by **Dec 2027**. Eclypsium+1
- CISA **2025 Minimum Elements for SBOM** (update to NTIA 2021). CISA+1
- FDA **June 2025** premarket cybersecurity guidance (SBOM included). U.S. Food and Drug Administration
- **SPDX**: ISO/IEC 5962:2021; v3.0/3.0.1. FOSSA+1
- **CycloneDX**: v1.6 (Apr 2024), **v1.7 (Oct 21, 2025)**; ECMA standardization reported. CycloneDX+2GitHub+2
- **CSAF v2.0** approved as ISO/IEC standard (May 20, 2025). OASIS Open
- VEX guidance & examples (CISA). CISA+1

Thank You

CRob_at_OpenSSF_dot_org

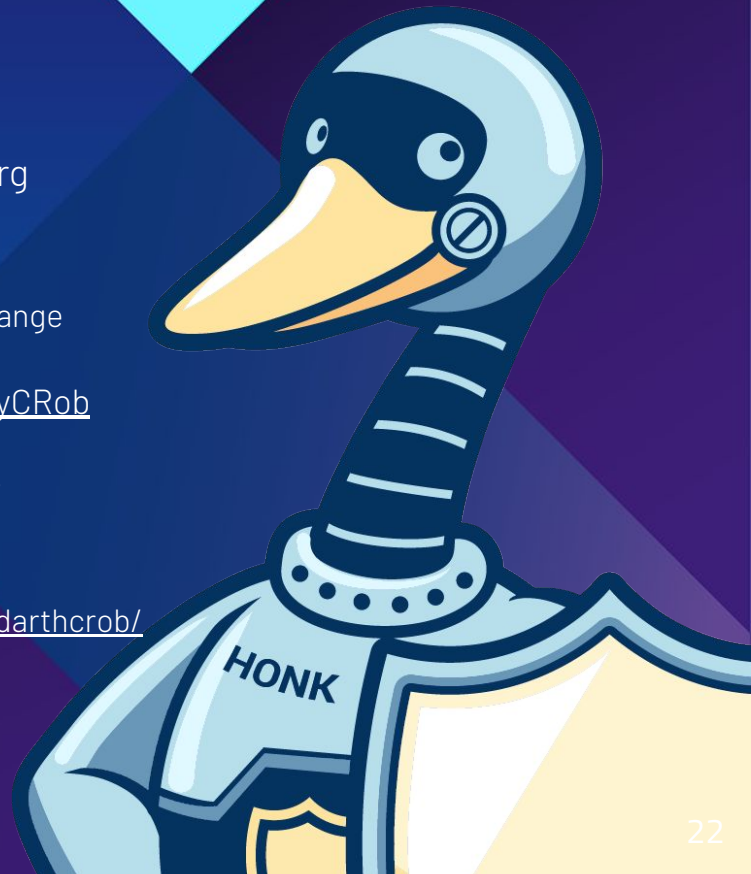
@~~SecurityCRob~~

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa
What's in the SOSS?

https://www.linkedin.com/in/darthcrob/



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Thank You

- X @openssf
- Bluesky OpenSSF
- LinkedIn OpenSSF
- Mastodon social.lfx.dev/@openssf
- YouTube OpenSSF
- Facebook OpenSSF

- Join a Working Group/Project
- Come to a Meeting (see Public Calendar)
- Collaborate on Slack
- Contribute on GitHub
- Become an Organizational Member
- Keep up to date by subscribing to the OpenSSF Mailing List

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Legal Notice