

The Evolving BOM Ecosystem: Navigating Hardware, Software, and Global Regulations

Cassie Crossley

CyBeats | Corporate Board Member
Advisory Board Chair
cassie@cybeats.com

Allan Friedman

Institute for Security and Technology
allan.friedman@gmail.com



Regulations & Frameworks Tracker

One authoritative, always-current reference for every SBOM and vulnerability management mandate that matters to you.

<https://cybeats.com/regulations>

Filter by Industry

10 sectors: Medical, ICS/OT, AI, Automotive & more

Filter by Region

12 countries — EU, US, Canada, Japan, China & more

Always Up to Date

Tracks effective dates, drafts, and emerging rules

The screenshot shows the Cybeats website's 'Regulations & Frameworks Tracker' page. The header includes the Cybeats logo and navigation links for Products, Resources, Company, and Investors, along with a 'Book a Demo' button. The main heading is 'Supply Chain Security Standards, Regulations and Frameworks Tracker'. Below this, a subtitle reads: 'Track and explore SBOM and vulnerability management regulations across industries and jurisdictions. Filter by country, market segment, and compliance status to find the requirements that matter to your organization.'

The interface features a search bar labeled 'Search regulations ...' and a status 'Showing all 87 regulations'. On the left, there are filters for 'Industry' (All, General, ICS/OT, Medical, Federal, AI, Rail, Automotive, Telecom, Financial, Aerospace) and 'Country/Region' (All, Global, US, EU). The main content area displays the 'EU Machinery Regulation (EU) 2023/1230' by the 'European Parliament and Council'. It includes a table with columns for Industry, Country, SBOM, and Vulnerability Management, with filters for General, EU, Implicit, and Implicit. The 'INTRODUCED' date is 'June 13, 2023' and the 'EFFECTIVE' date is 'January 19, 2027'. Below this, there are sections for 'SBOM NOTES' and 'SBOM-ADJACENT PROVISIONS'. The 'SBOM NOTES' section states: 'Regulation (EU) 2023/1230 on machinery (consolidated 29 June 2023, 126 pages). Replaces Directive 2006/42/EC. Applies generally from **20 January 2027**. The text does **not** explicitly mention SBOM, Software Bill of Materials, CycloneDX, SPDX, or VEX. Classification is **Implicit** because the regulation treats safety-critical software as a first-class object with transparency and identification requirements.' The 'SBOM-ADJACENT PROVISIONS' section includes a bullet point for 'Annex III 1.1.9 (Protection against corruption)' which states: 'The machinery or related product shall identify the software installed on it that is necessary for it to operate safely, and shall be able to provide that information at all times in an easily accessible form' - a direct software-inventory requirement for safety-critical software.'

Free resource · No login required · Links to official sources

Global Regulations Are Expanding BOM Expectations

REGULATION	FOCUS	BOM / EVIDENCE	UNIQUE REQUIREMENT
EU CRA	Product cybersecurity	SBOM, VEX, vuln handling evidence	Post-market obligations
FDA Cybersecurity	Medical devices	SBOM	Secure updateability
EU AI Act	AI transparency	AIBOM, model documentation	Training data & GPAI traceability
NIST SSDF	Secure development	Process evidence	Operational practices
ISO 42001	AI governance	AI inventory / provenance	Organizational governance
Canada ADM	Government AI	Algorithmic transparency	Impact assessments
JC-STAR	IoT assurance	Device/software inventory	Labeling & assurance levels

The world is not converging on one BOM format. It is converging on evidence-backed transparency.

EU CRA

Reg. 2024/2847

CEN/CENELEC

Mandate accepted

JTC 13 / WG9

EN 40000-1-X

prEN 40000-1-3

SBOM · HBOM · Vuln

EN 40000-1-3

Final · Summer 2026

INTERIM BRIDGE

BSI TR-03183-2 v2.0

§5.1: Recursive dependency resolution — each path downward. The first external component outside your delivery scope must be fully identified.

SOFTWARE BILL OF MATERIALS (SBOM)

HARDWARE BILL OF MATERIALS (HBOM)



Accepted Formats

CycloneDX · SPDX

Explicitly named in prEN 40000-1-3



Hardware Inventory

PRE-8-RQ-01 / 02

All physical + silicon components documented.



Depth of Visibility

Top-level minimum.

Full transitive tracking strongly recommended.



Vulnerability Mapping

RCP-4-RQ-01

Hardware CVEs tracked with same urgency as software.



Keep for 10 Years

Annex VII · Article 13

Available to surveillance authorities — 10 yrs or support period.

What Must Be Inventoried

Silicon / Chips

CPUs · SoCs · FPGAs

Physical Parts

PCBs · modules

Firmware

BSPs · bootloaders

Annex VII

Article 13

BSI §5.1

PRE-8-RQ-01

PRE-8-RQ-02

RCP-4-RQ-01



ADM Directive

Federal AI governance

AIDA

High-impact AI law

AIA Level III

High impact · BOM req'd

AIA Level IV

Critical · BOM mandatory

CPCSC 2026

Signed SBOM in contracts

Software & Environment

A

Traditional SBOM

- SPDX · CycloneDX
- Libraries · OS deps · Docker layers
- Expose Vulnerabilities

Procurement

- BOM = first doc in Crown audit
- CPCSC Level 1+ from Summer 2026
- Cryptographic SBOM signing required

Data Cluster

B

Data-BOM

- Training · Validation · Test datasets
- Bias metadata · Fairness (AIDA)
- Sources · Curation · Lineage

Implementation

- JSON / XML — no PDF-only BOMs
- Update on retrain or dep change
- VEX file alongside BOM (no CVE fatigue)

Model Cluster

C

Model Card / Model-BOM

- Architecture · Hyperparameters · Metrics
- Agentic AI: tool-use boundaries documented
- Performance benchmarks per deployment

Global Alignment

- US NIST SP 800-218 (SSDF)
- EU EU CRA — MRA in progress
- G7 AI SBOM Guidance May 2026

1 STAR**Basic / Low**

Passwords
Identity
Anti-intrusion

Self-declaration

2 STAR**Moderate**

Firmware updates
Port management
Data protection

Self-declaration

3 STAR**SBOM****High**

Log management
Access controls
Supply chain security

3rd-party assessment

4 STAR**SBOM****Critical**

Full lifecycle design
SBOM mandatory
Independent verification

3rd-party assessment

BOM Requirements**METI SBOM Guidance 2.0**

SPDX · CycloneDX
Machine-readable mandate

Gov Procurement 2026

Level 2+ · Network cameras
SBOM evidence required

Energy Grid · April 2027

Level 1+ · PV & storage
Higher levels expected

Global Alignment**JP Japan JC-STAR**

IoT labeling scheme · IPA/METI

US US Cyber Trust Mark

NIST IoT cybersecurity baseline

EU EU Cyber Resilience Act

MRA negotiations underway

MRA · JC-STAR ≈ CRA compliance expected

New in 2026**G7 AI SBOM Guidance**

May 2026 · Japan + US + EU
"Minimum Elements for AI SBOM"

Key References

IPA JC-STAR Portal
METI SBOM Guidelines
G7 Joint Guidance May 2026

What Belongs Where?

Transparency artifacts across the AI and agentic stack

ARTIFACT	CAPTURES	EXAMPLE
SBOM	Software dependencies, containers, libraries, licenses, CVEs	Python libs, container image, app framework
CBOM	Cryptographic assets, algorithms, keys, certificates, crypto libraries	TLS certificates, signing keys, HSM-backed keys, crypto modules
HBOM	Hardware components, devices, firmware, platform parts, provenance	GPU, TPU, accelerator cards, servers, drivers
AIBOM / ML-BOM	Model, dataset, training/eval metadata, model card, provenance	Base model, adapter, dataset source, eval metrics
Agentic System BOM	SBOM + AIBOM + Runtime + Behaviours	Tools, MCP servers, prompts, policies, memory, identity bindings
Runtime evidence	What actually happened and what was used	Tool calls, approvals, denied actions, traces, eval results

Current AIBOM covers the AI/ML layer. A broader agentic system inventory links AIBOM with software, cryptography, hardware, and evidence artifacts.

AIBOM Initiative

OWASP GenAI Security Project — open source AI supply chain transparency

What it is: Open AIBOM Generator

Open source tool for generating AIBOMs. Introduced at RSAC 2025 by Helen Oakley (SAP) and Dmitry Raidman (CyBeats).

What it does: Real models, real metadata

Generates CycloneDX 1.6 AIBOMs for Hugging Face models. Mappings to SPDX 3.0 AI Profile in flight.

Where to run it: Live today

Open source on GitHub. Runnable demo and API on Hugging Face Space. Listed in the CycloneDX Tool Center for immediate enterprise use.

2026 Roadmap: Expansion

Tighter field checks, automated extraction at release cadence, and the AIBOM Generation Handbook with citeable procurement language.



GenAI-Security-
Project /
aibom-generator
genai.owasp.org /
owasp-aibom

<https://huggingface.co/spaces/GenAISecurityProject/OWASP-AIBOM-Generator>



AIBOM languages and how they differ

CycloneDX (v1.5 - 1.7) ML-BOM

STRONGER

Native ML types, fast iteration, broader industry support from open source and commercial tools.

WEAKER

Fewer AI metadata fields than SPDX. No native equivalent for sensitive PII, explainability, autonomy, safety risk.

SPDX (3.0.1) AI Profile

STRONGER

Deepest AI metadata (explainability, energy, sensitive PII, safety risk), formal trainedOn/testedOn relationships.

WEAKER

AI tooling still maturing (Released Dec 2024). JSON-LD/RDF format less ergonomic for CI/CD engineers.

AIBOM languages and how they differ

CycloneDX (v1.5 - 1.7) ML-BOM

STANDARD: ECMA-424

ADOPTION

Leads in security and DevOps tooling. Has simple documentation and SBOMs are more human readable and editable.

NEXT

2.0 in development, due June 2026.

SPDX (3.0.1) AI Profile

STANDARD: ISO/IEC 5962:2021

ADOPTION

Leads in legal, compliance, OS distributions like Zephyr and Microsoft. Introduced multiple breaking changes along the way.

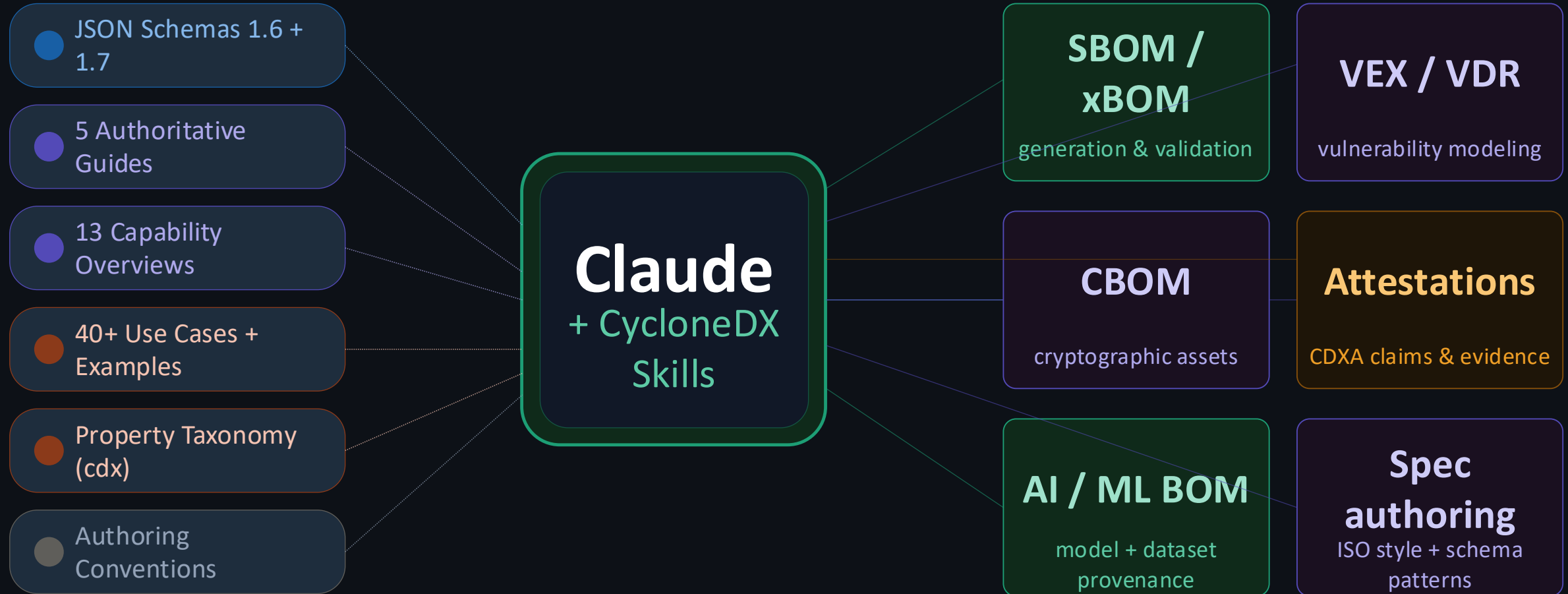
NEXT

3.1 release candidate in active development.

CycloneDX Skills for Claude

github.com/CycloneDX/skills · Apache 2.0 *Install once. Claude becomes a CycloneDX expert.*

SKILL BUNDLES



```
$ download cyclonedx-spec.skill
$ install in Claude → expert-level guidance on every CycloneDX BOM type
```



OWASP TEA

Transparency Exchange API • OWASP / ECMA TC54 • Beta 2

A standard API for automated discovery and exchange of supply chain transparency artifacts and intelligence

What it does

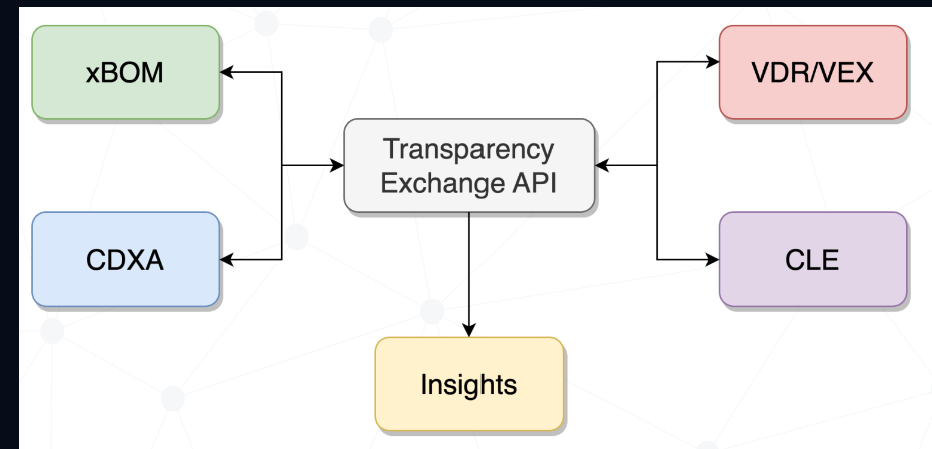
Automates discovery and retrieval of supply chain transparency artifacts from upstream vendors. Consumers query once and stay current as artifacts update.

Status & standards

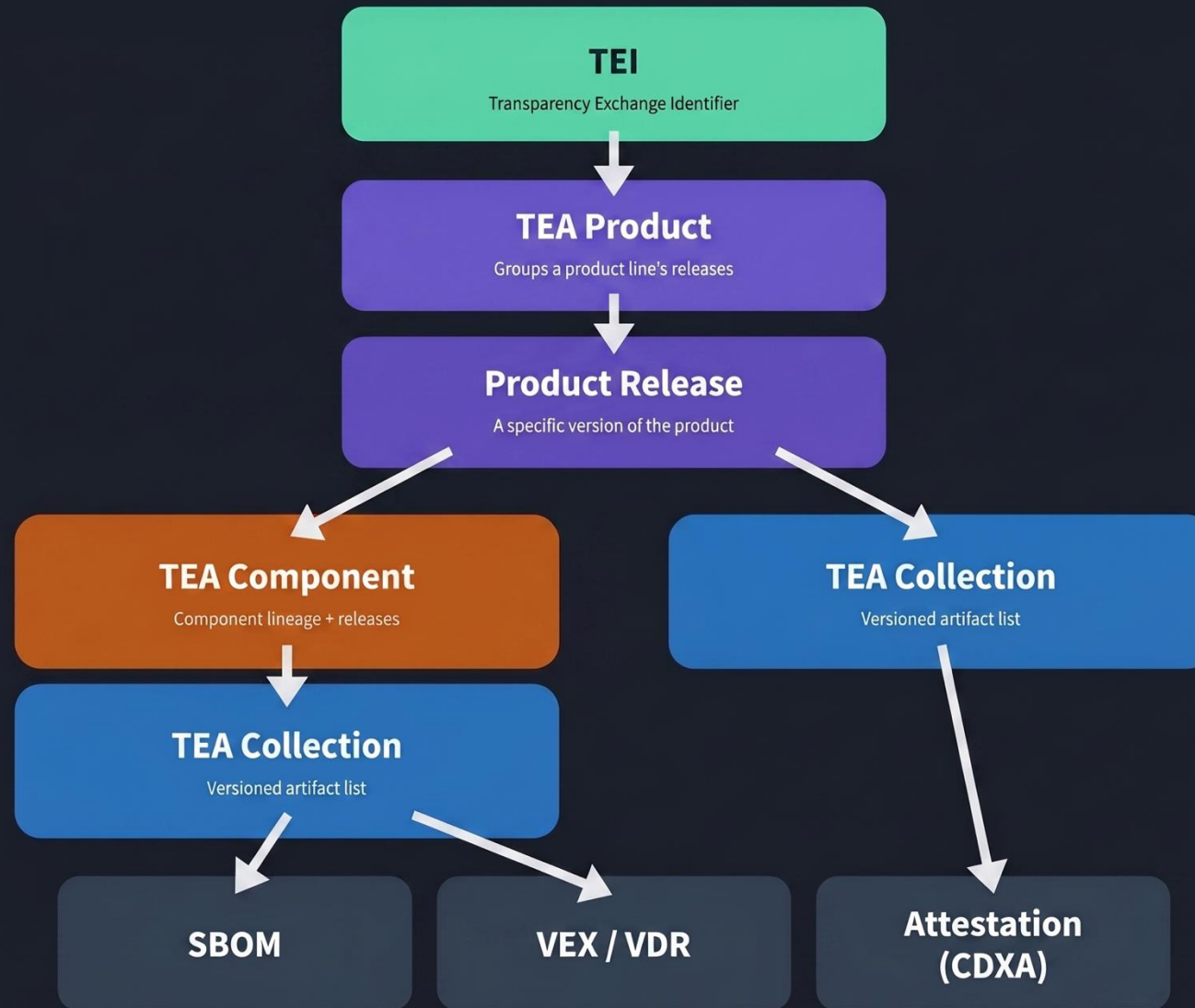
Beta 2: consumer API ready-to-implement
Publisher API follows 1.0 release
Governed by ECMA TC54 tg1
Apache 2.0 • 99 stars • 17 forks

Artifact types supported

SBOM, HBOM, AIBOM, CBOM, SaaSBOM
VEX, VDR (format-agnostic)
Attestations (CDXA)
Product lifecycle events (ECMA-428 CLE)



OWASP TEA Data Model



New Working Group: ISA 62443 Supply Chain Security

What it is

A new ISA standard for assessing supply chain security trustworthiness and transparency — modeled on ISA/IEC 62443-4-1 and grounded in the MITRE System of Trust framework.

Scope

- Suppliers
- System integrators
- Asset owners

Each link assessed individually; shared responsibility across the industrial ecosystem.

Why it matters

Gives industry a common language of trust: understandable to regulators, meaningful to asset owners, actionable for suppliers and integrators.

Volunteers wanted — help shape this standard

Contact: Alex Boesenberg, Manager of Advocacy,
International Society of Automation

aboesenberg@isa.org • 571-275-9309

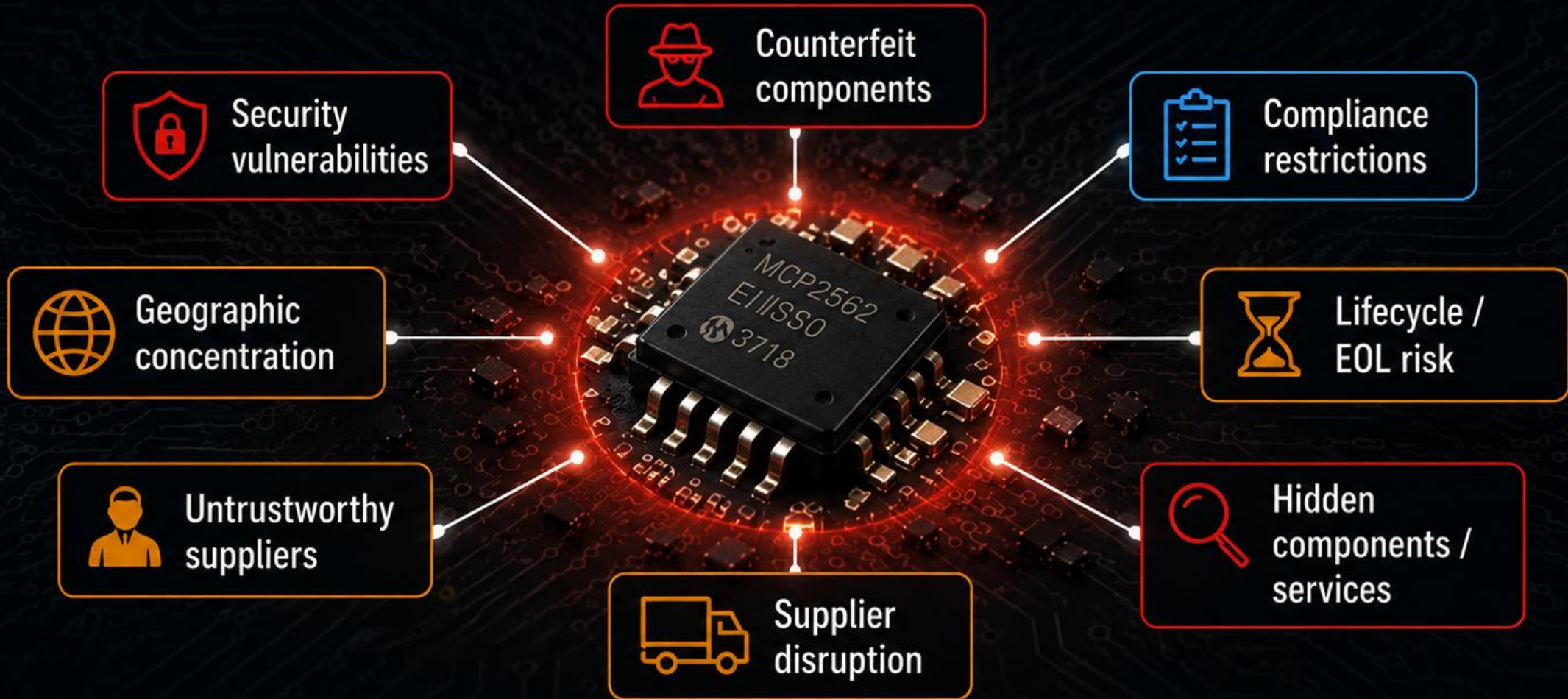


HBOM Today

- Hardware supply chain transparency is important, urgent, and inevitable.
- Existing BOMs do not support assurance, response, or auditability
- HBOM is coming through policy, contracts, and customer expectations
- Industry has a narrow window to shape how this works in practice

ONE COMPONENT, MANY RISKS

HARDWARE SUPPLY CHAIN RISK



Hardware supply chain risk is not one problem. It is many different problems that all depend on understanding what components are present and where they are used.

Hardware supply chain risk is already operational



Energy

Solar inverter concerns



Transportation

Connected buses



Defense

Obsolete and counterfeit parts



Logistics

Port cranes



Telecommunications

Trusted supplier restrictions



Automotive

Semiconductor shortages



Healthcare

Long-lived medical devices

These cases differ technically and politically, but all depend on understanding hardware components, suppliers, and dependencies

Hardware provenance requirements are already appearing across sectors.

- Explicit HBOM Requirements TODAY
 - FCC Router Conditional Approval
 - Golden Dome requirements
 - DOD 5G Procurement
- Attestations about specific attributes
 - Section 5949 – Three specific semiconductor manufacturers
 - Section 889 – Telecommunication vendor bans
 - FAR 52.240-1 – Unmanned Aircraft Systems and components
- Implicit Requirements or Suggestions
 - Cyber Resilience Act – Hardware inventories for vulnerability management
 - BIS Connected Vehicle Rule
 - CSRIC VII - “industry should consider HBOM”

Manufacturing BOM vs HBOM

Design BOM

Attestations

Component Data

Manufacturing BOM

HBOM

- Built to manufacture products
- Focused on assembly and procurement
- Often proprietary and siloed
- Tracks parts required for assembly
- Optimized for factories and ERP systems
- May stop at direct suppliers

- Built to understand risk and provenance
- Focused on traceability and assurance
- Intended for *controlled* sharing
- Tracks components relevant to security, resilience, and compliance
- Optimized for analysis and decision-making
- Often requires deeper supply chain visibility

“a structured, machine-processable representation of electronic components, subsystems, and provenance information that make up a hardware product, enabling identification, assessment, and management of risks associated with hardware supply chain”.

SBOM vs. HBOM

Similarities

- **Ecosystem lessons**
 - Existing services and practices
 - Diverse base → diverse perspectives
 - Emerging standards
 - No one-size-fits all
- **Governance challenges**
 - Concerns about IP
 - Specifications vs Requirements
 - Value in having one; need capacity to use it
- **Operational realities**
 - *Separate data from risk*
 - Cross-sector applicability
 - Complex & varied manufacturer ecosystem

Differences

- **Supply chain complexity**
 - Longer, more opaque supply chains
 - Longer tail of deployed systems
 - More expensive verification
- **Policy and trust**
 - More direct government interests
 - Greater confidentiality concerns
 - Levels of assurance
- **Risk Model Differences**
 - Compliance-driven use cases
 - Different risk models
 - Response & mitigation to risks
 - Geography and flags matter

HBOM can learn from SBOM, but hardware changes the economics, incentives, and trust models.

Where is HBOM today?

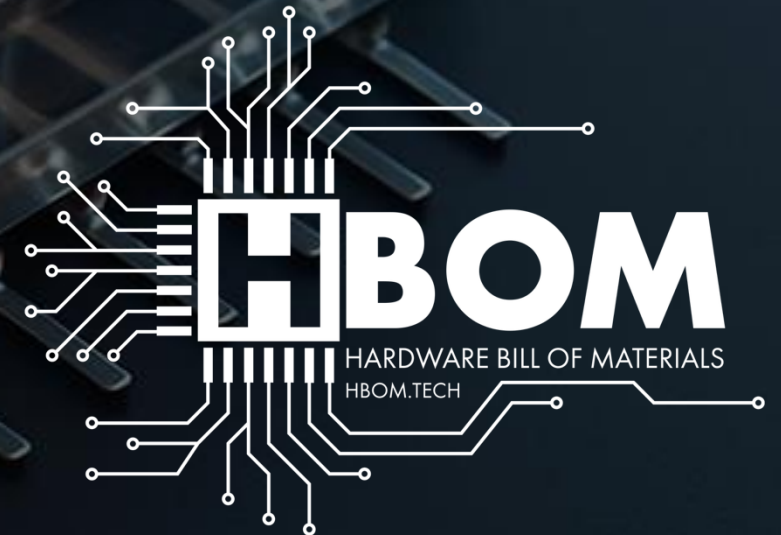


Existing HBOM efforts provide an important foundation, but broader **cross-sector coordination and security-focused implementation work is still needed.**



What Will a Successful HBOM Ecosystem Require?

- Shared definitions and scope for hardware and semiconductor provenance
- Alignment across existing standards, tools, and sector-specific approaches
- Adaptable levels of assurance for different risk profiles and operational needs
- Trusted mechanisms for attestations and protection of sensitive data
- A practical roadmap for implementation and interoperability across processes and sectors



Q&A

Cassie Crossley

CyBeats | Corporate Board Member Advisory Board Chair
[/linkedin/in/cassiecrossley](#)
cassie@cybeats.com

Allan Friedman

Institute for Security and Technology
[/linkedin.com/in/allanafriedman/](#)
allan.friedman@gmail.com