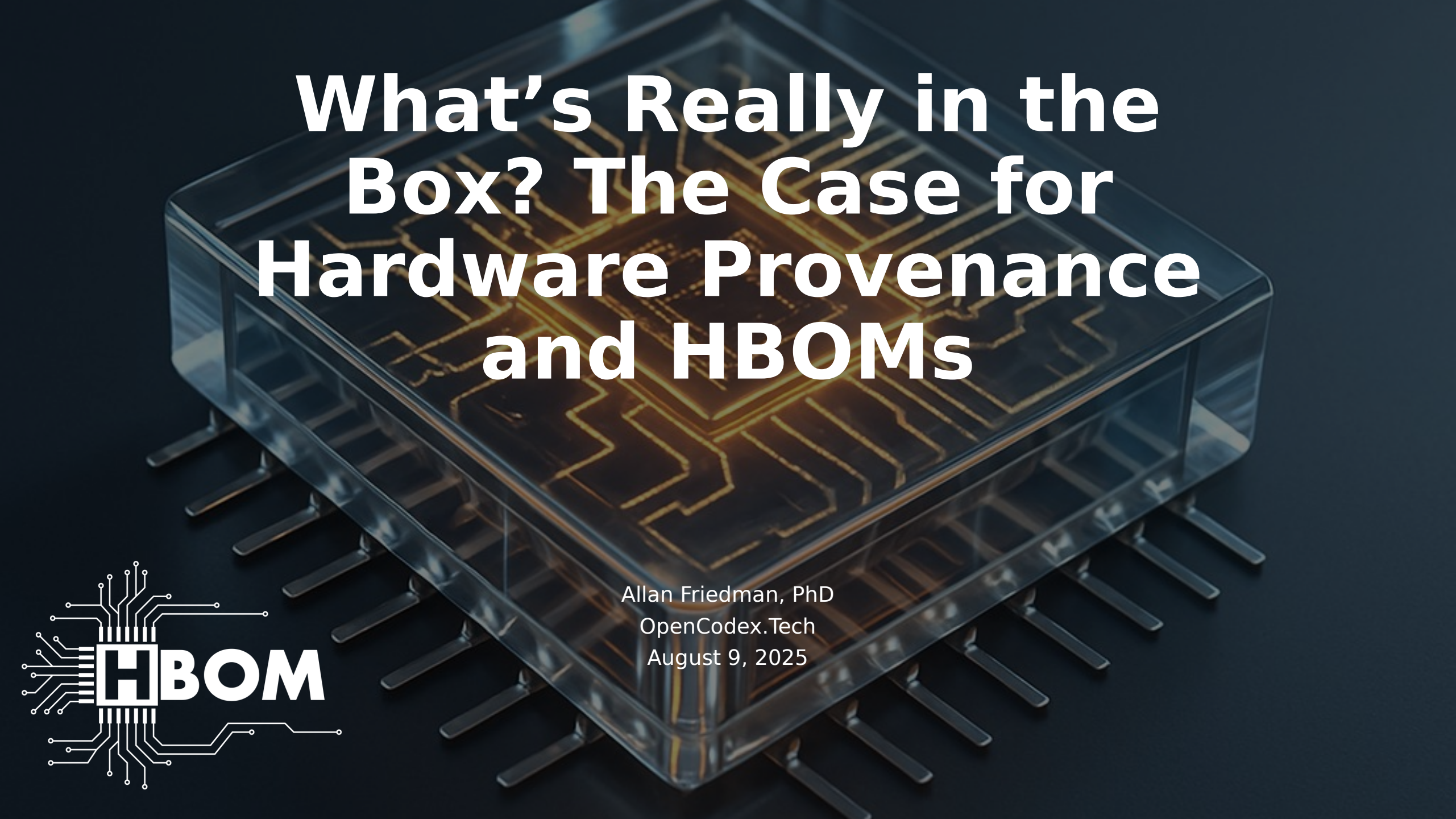
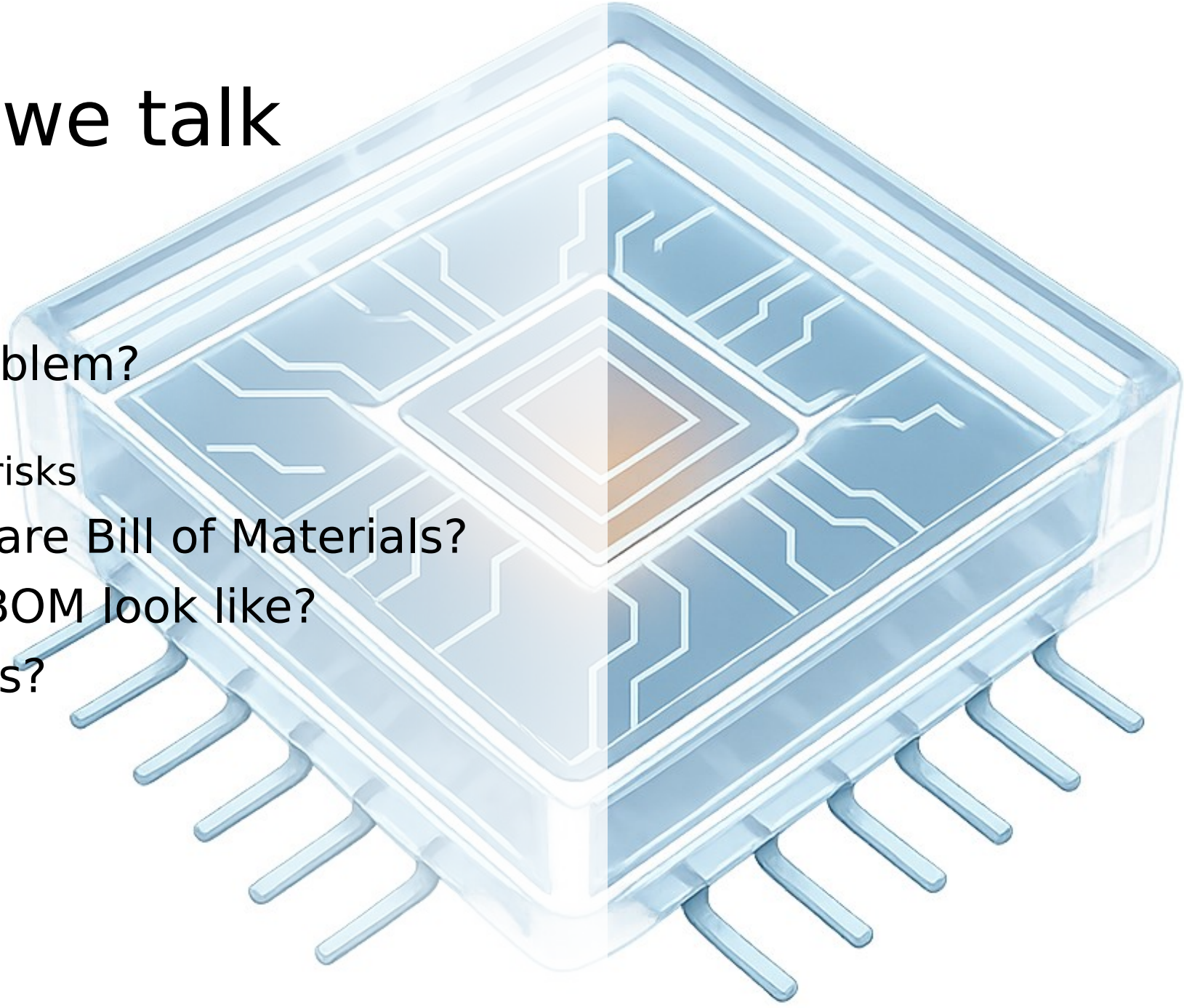
# What's Really in the Box? The Case for Hardware Provenance and HBOMs




Allan Friedman, PhD
OpenCodex.Tech
August 9, 2025

# What will we talk about?

- What’s the problem?
  - Supply chains
  - Supply chain risks
- What is Hardware Bill of Materials?
- What might HBOM look like?
- Why not do this?



- Risks
- Percieved
- Why shouldn’t we do this?

Forbes

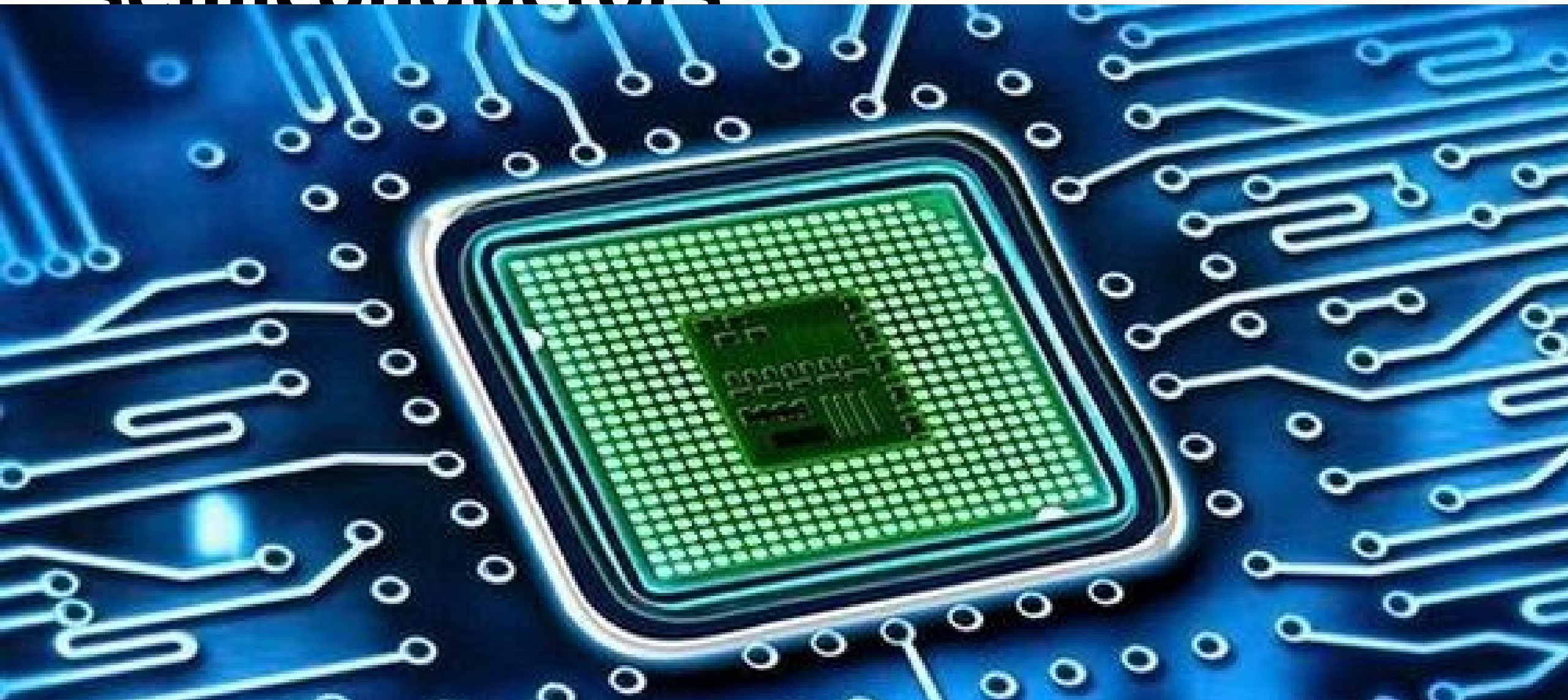
DAILY COVER

# Silicon Valley's Military Drone Companies Have A Serious 'Made In China' Problem

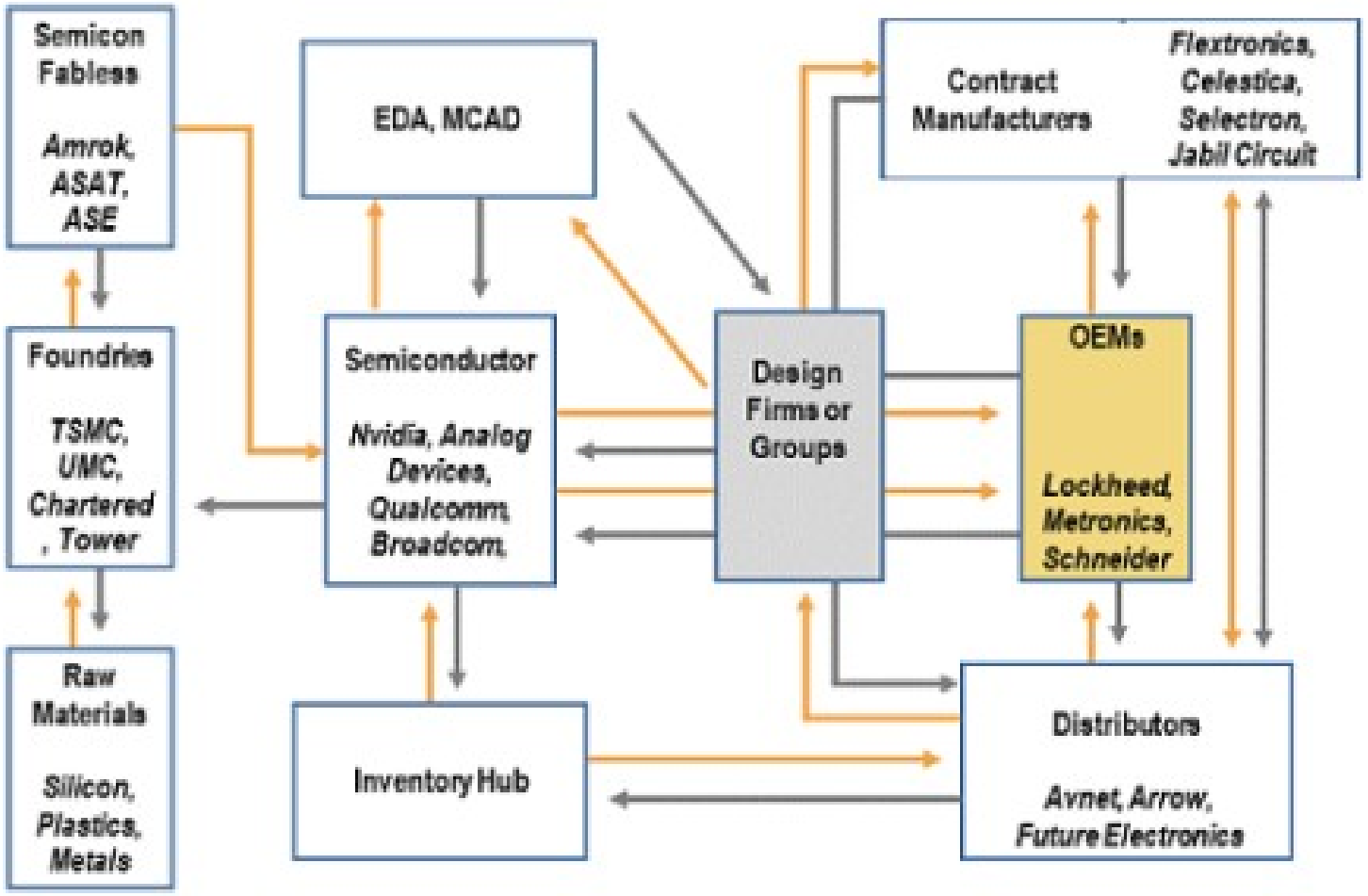
By David Jeans, Forbes Staff. Senior writer covering tech, defense

Apr 16, 2025, 06:30am EDT, Updated Apr 17, 2025, 01:31am EDT

# We’re going to have to pay a lot more attention to our semiconductors



# Electronics Supply Chain




Anew-da.com

# Good News – Can’t build a THING without a BOM

## Manufacturing BOMs

- Logistics chains have always been a part of manufacturing
- Modernization has pushed for greater efficiency
- Quality requires data and effective management

# Missing: Provenance

# Counterfeits

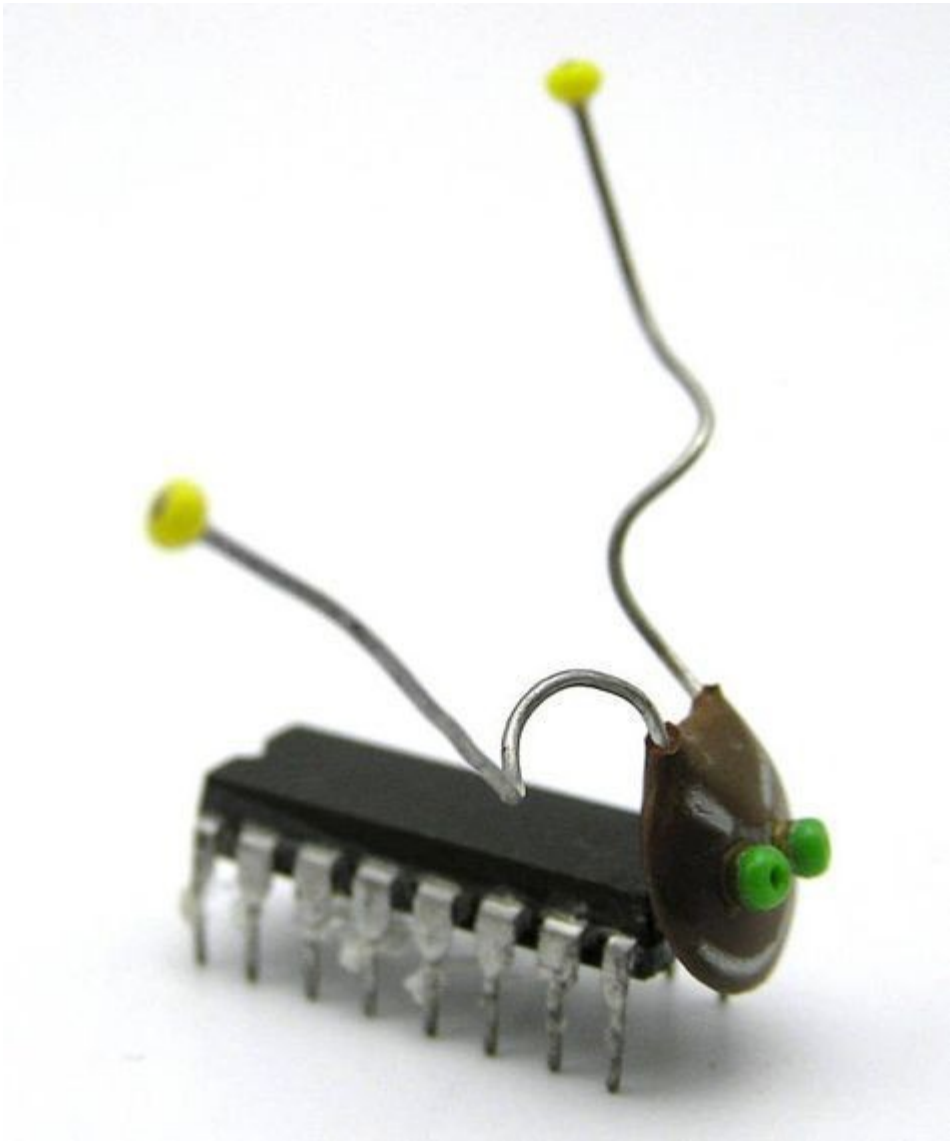
# Counterfeits

## Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts

WASHINGTON -- A Senate Armed Services Committee investigation discovered counterfeit electronic parts from China in the Air Force's largest cargo plane, in assemblies intended for Special Operations helicopters, and in a Navy surveillance plane among 1,800 cases of bogus parts, a committee report released today [PDF 1.44 MB] shows.

# Vulnerabilities

- Downfall
- Augury
- LeftoverLocals
- GhostRace
- TikTag



# Critical Chipset Bugs Open Millions of Android Devices to Remote Spying

Apr 21, 2022 Ravie Lakshmanan

Three security vulnerabilities have been disclosed in the audio decoders of Qualcomm and MediaTek chips that, if left unresolved, could allow an adversary to remotely gain access to media and audio conversations from affected mobile devices.

According to Israeli cybersecurity company Check Point, the issues could be used as a launchpad to carry out remote code execution (RCE) attacks simply by sending a specially crafted audio file.

# Active Tampering

# The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

# Well… sometimes attacks are overstated

This article is more than **1 year old**

## Forgotten that Chinese spy chip story? We haven't – it's still wrong, Super Micro tells SEC

Server maker drags Bloomberg in note to customers, watchdog, still checking its motherboards

Kieren McCarthy

Mon 22 Oct 2018 // 19:20 UTC

# Rogue communication devices found in Chinese solar power inverters

By **Sarah Mcfarlane**

May 14, 2025 9:55 AM PDT · Updated May 14, 2025

# Countries matter

- **FOCI**
- **Compliance**
  - **Sanctions**
  - **Regulations**
  - **Tariffs**
  - **Import/Export controls**

Forbes

DAILY COVER

# Silicon Valley's Military Drone Companies Have A Serious 'Made In China' Problem

By David Jeans, Forbes Staff. Senior writer covering tech, defense

Apr 16, 2025, 06:30am EDT, Updated Apr 17, 2025, 01:31am EDT

# Gubmints gonna Gubmint

# Gubmints gonna Gubmint

- Regulations are **here**

- BIS automotive rules
- Telecommunications Rules
- FDA
- Tariffs
- Export controls
- NDAA Section 5949

# Policies are coming

- “Long, opaque supply chains leave gaps that can too easily be exploited, and we need a strategy for closing them in close collaboration with our allies.”
- Seth Moulton

**BIS connected vehicle rule**

- Jan 2029
- Originally called for an HBOM
- formal record the supply chain relationships of parts, assemblies, and components required to create a physical product, including information identifying the manufacturer, and related firmware
- a formal record containing the details and supply chain relationships of various components used in building software

# BIS connected vehicle rule

# Goals of HBOM: Supply Chain Visibility

*Tracking across the supply chain down to customers or pre-sale regulatory compliance*

- Consistent and repeatable
- Reliable and predictable
- Portable
- Automatable
- Auditable

# Scope

Security domain

Provide metadata to make decisions about the origins and security risks of a given product

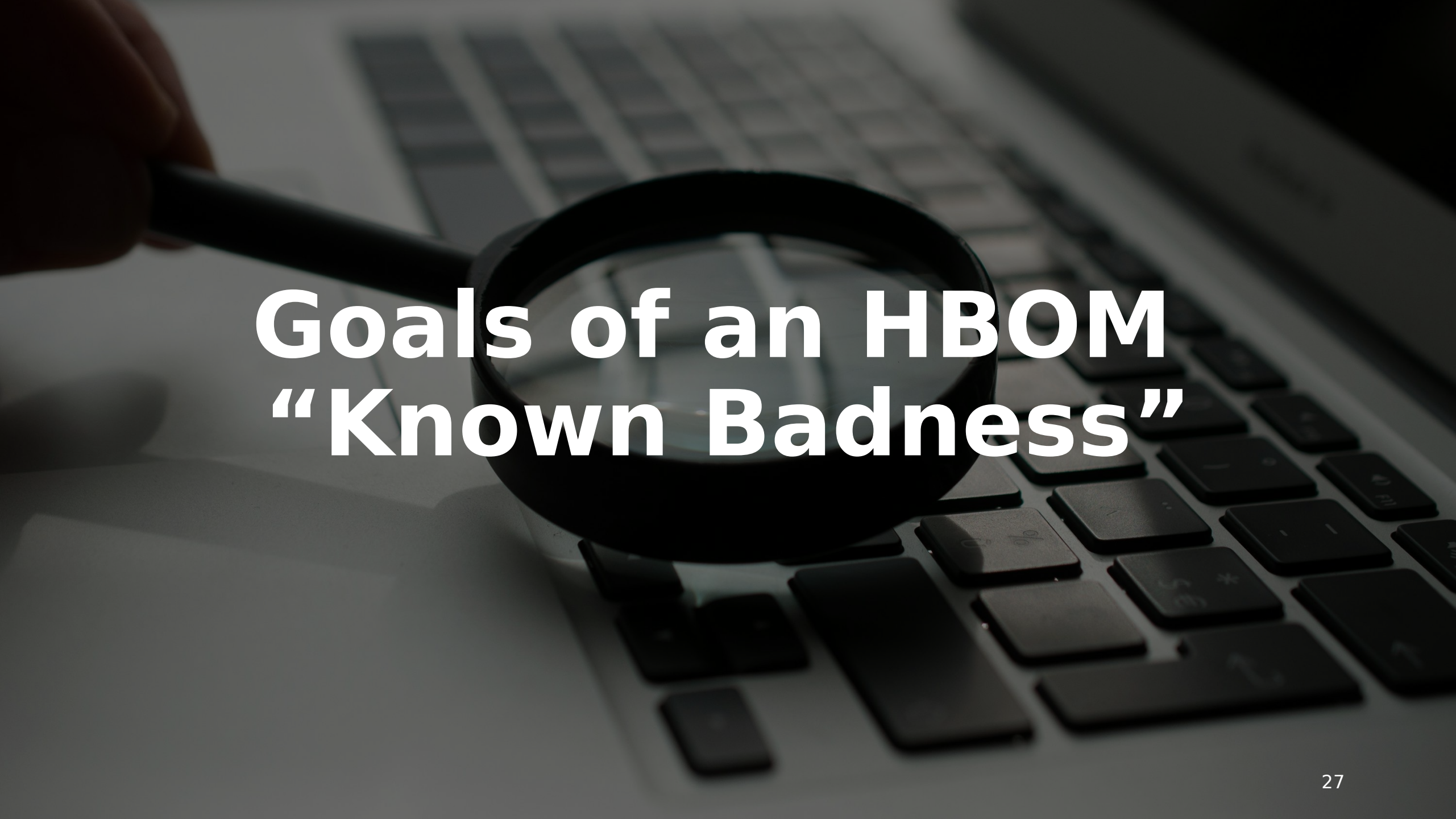
Semiconductors

Digital components

“store, process, transmit”

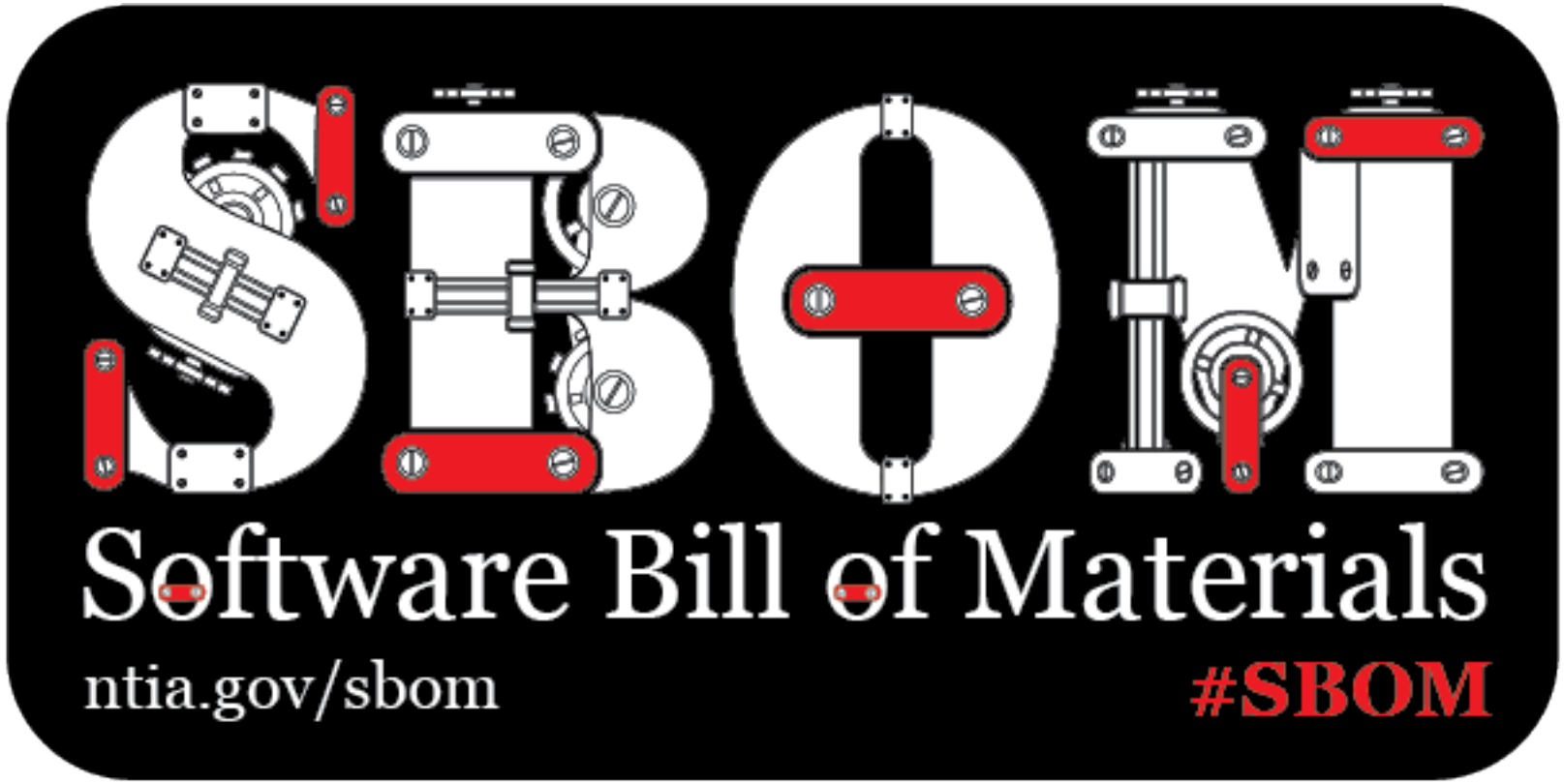
Not focusing on other supply chain topics

But need to be able to integrate with those efforts

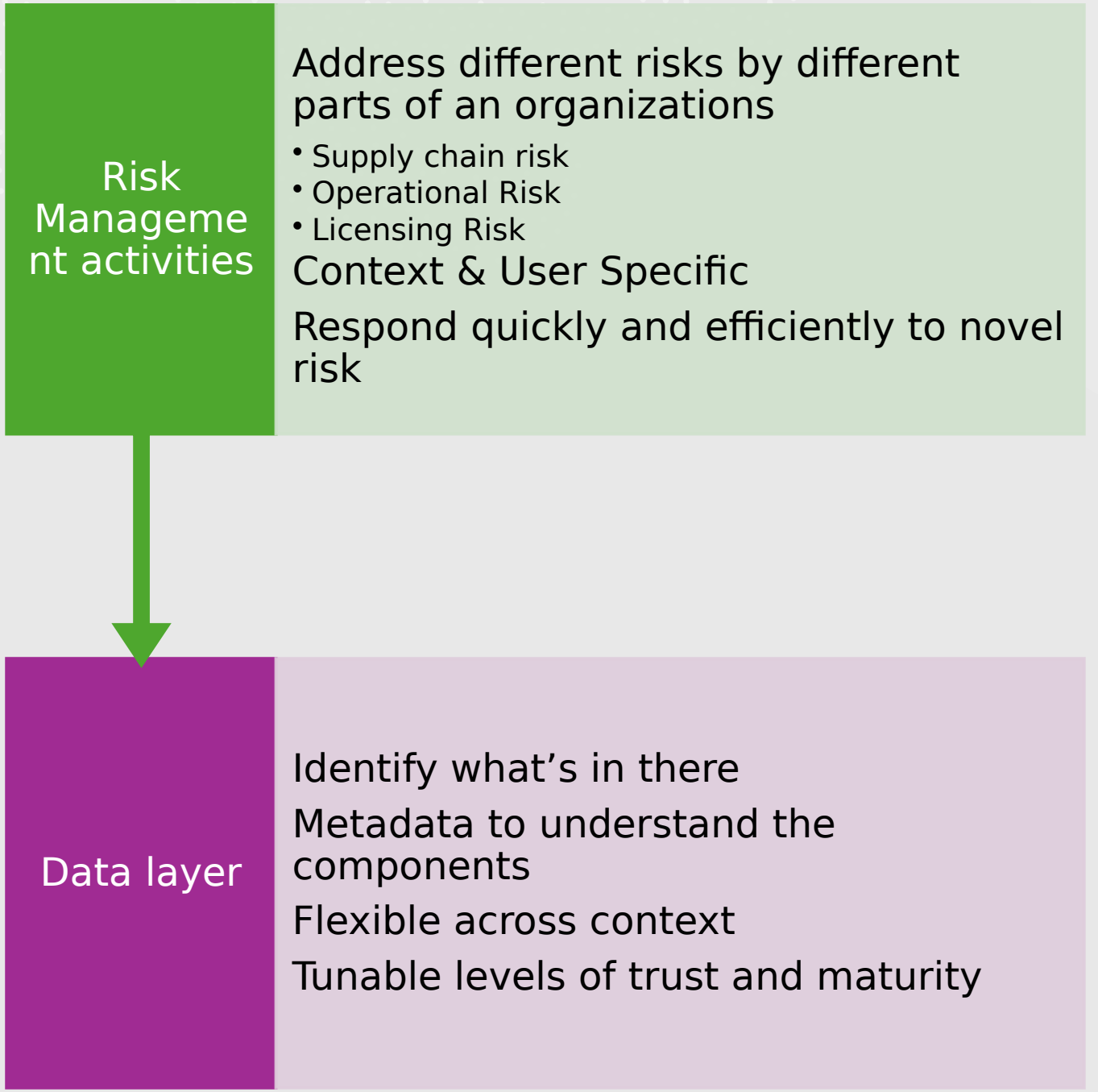


# Goals of an HBOM “Known Badness”

CISA
SBOM
CISA.GOV/SBOM


SBOM
Software Bill of Materials
ntia.gov/sbom
#SBOM

# BOM data as a separate transparency layer

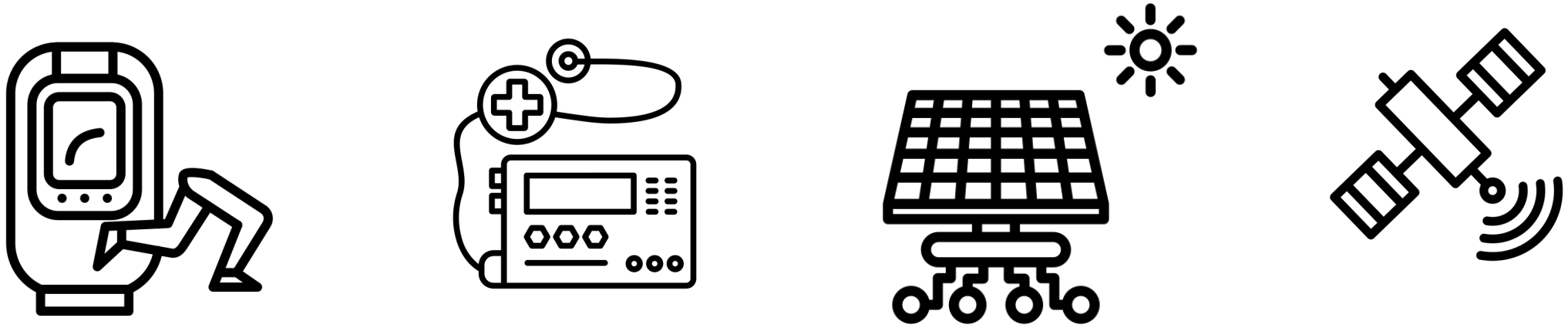


# Importance of a transparency layer

- Common approach to tracking data
- Plan for interoperability of standards
- Build in business processes
- Separate data from policy
- **Transparency is the first step - and often the most valuable**

# Who touched it? Who Could have?

# Levels of assurance



Governments will play a
but we can nudge them
strategically

# Cross sector Planning for HBOM

- Defense
- Critical Infrastructure
- Telecommunications
- Automotive
- Medical Devices

# Red teaming HBOM: Why not do this?

# SBOM vs. HBOM

**Similarities**

- Separate data from risk
- Existing services and practices
- Need for diverse base
- Concerns about IP
- Nascent standards
- No one-size-fits-all
- Many manufacturers

**Differences**

- Compliance-driven use cases
- Longer supply chains
- More expensive verification
- More direct government interests
- Different risk models

# Starting Point: An HBOM Framework

*Published by CISA's National Risk Management Center & Communications and IT Sector Coordinating Councils in 2023*

- Describes manufactured goods made up of assemblies comprising components
- Offers a set of basic roles for actors in the supply chain
- Presents a simple taxonomy of field names and basic details

# Explicitly Documented Use Cases

| | |
|---|---|
| Compliance | • Government<br>• Customer requirements<br>• Internal quality controls |
| Security | • Risks from entities and jurisdictions<br>• Component risks |
| Availability | • World events<br>• Clustering and concentration |

# Gaps

- Linking HW and SW
- Provenance
- Trust
- Measurement and auditing
- Specific implementations

# Integrating into existing efforts and standards

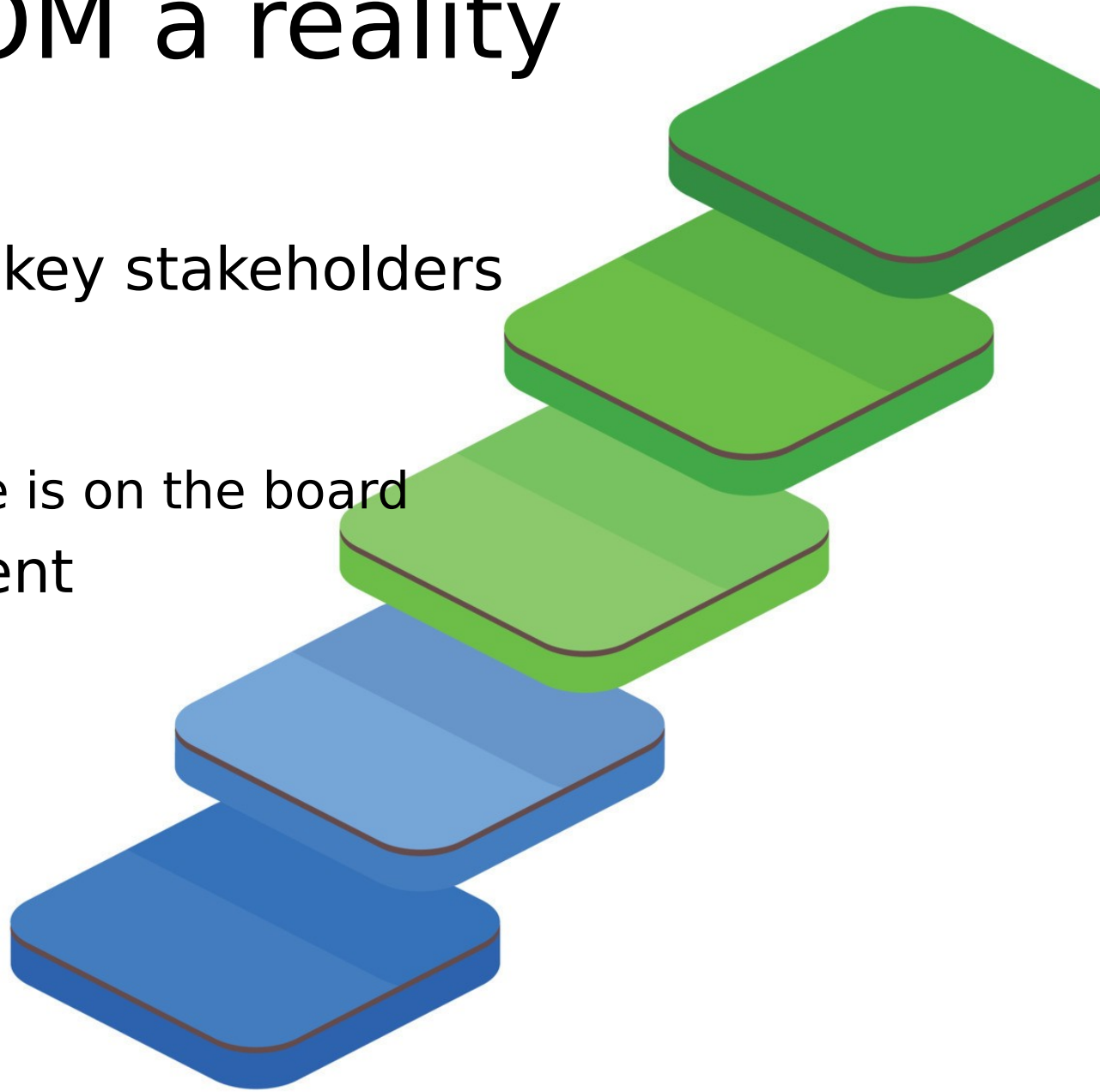
- CycloneDX BOM specifications
- SPDX Hardware-specific HBOM model
- Trusted Computing Group’s Platform Certificates
- Proprietary standards from enterprises and supply chain experts

# Identifiers

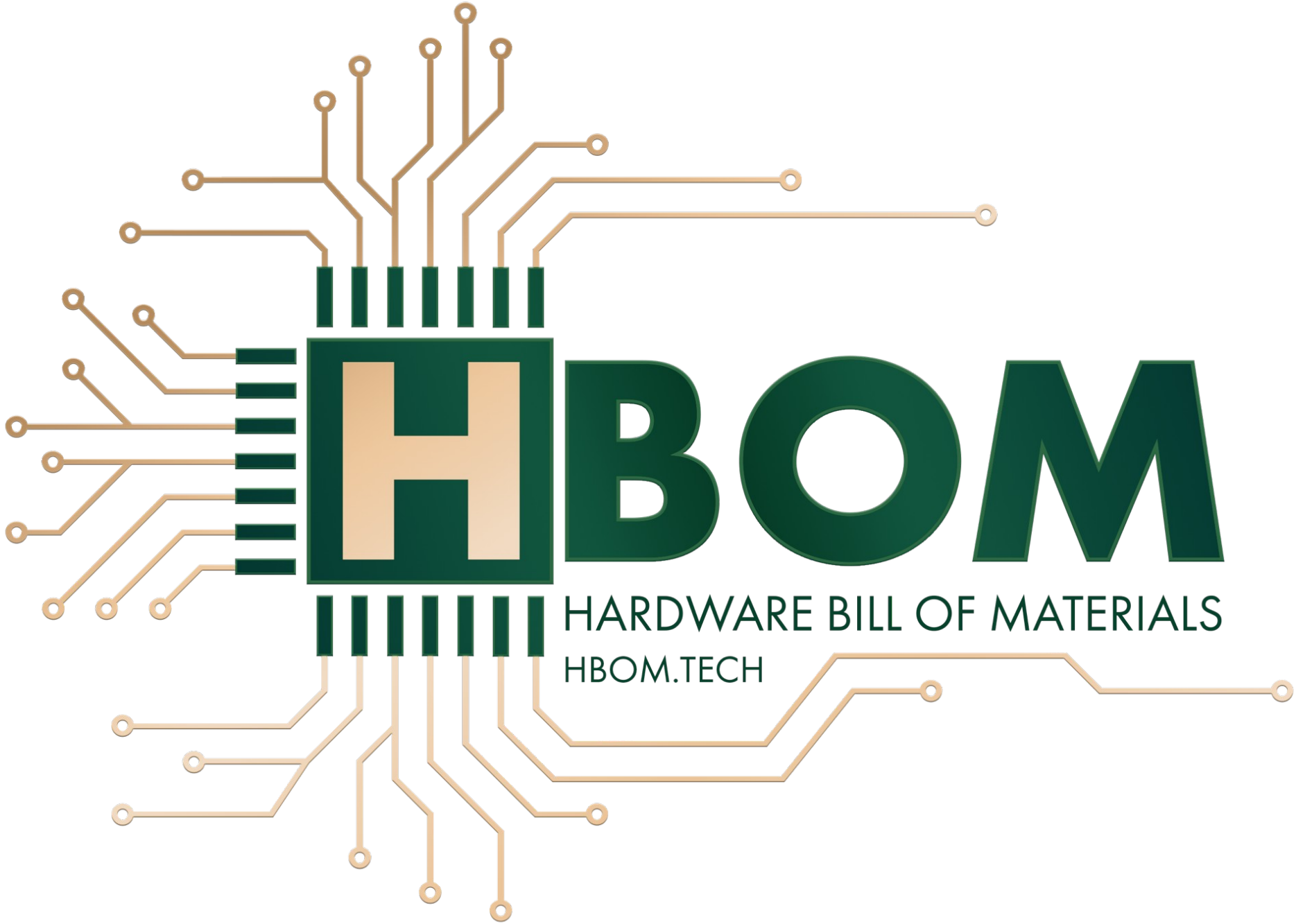
- Global identifiers are a hard problem.
  - SKU / lots / relabeling
  - We don’t even have them for software
- Numerous existing naming schema are used widely
- AI might be able to help

# Steps to make HBOM a reality

- Institutional home
- Funding – initially raised from key stakeholders
- Individuals
  - Pain points
  - Existing practices and what else is on the board
- Shared information environment
- Convening
  - It will be messy
- Decompose the problem with working groups
- Nudges – US policy



Would this be a good fit?


HBOM
HARDWARE BILL OF MATERIALS
HBOM.TECH