IAITAM ACE

May 7–9, 2024 The M Resort Las Vegas, NV

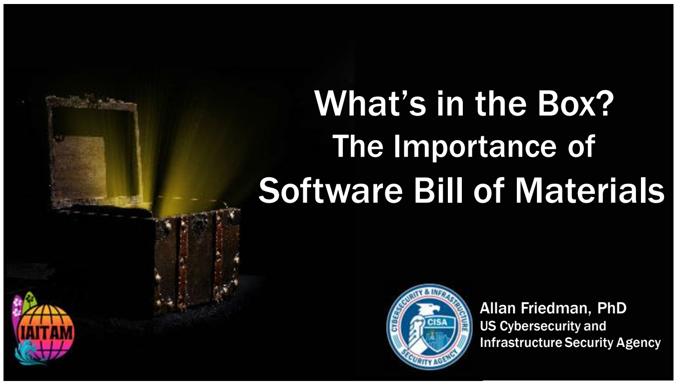
What's in the Box?

The Importance of Software Bill of Materials

Allan Friedman, PhD
US Cybersecurity & Infrastructure Security Agency

Finding your IAITAM Oasis

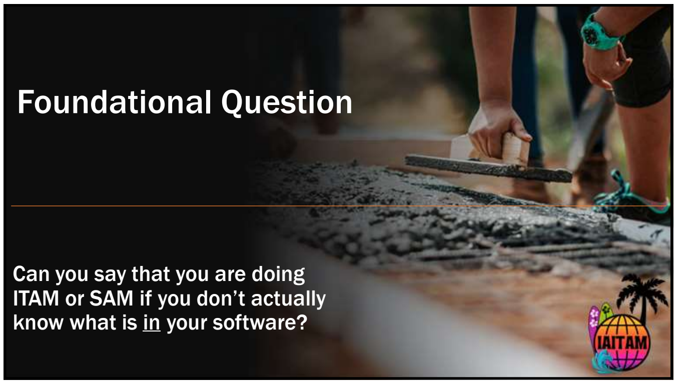
1



What's in the Box?
The Importance of
Software Bill of Materials

Allan Friedman, PhD
US Cybersecurity and
Infrastructure Security Agency

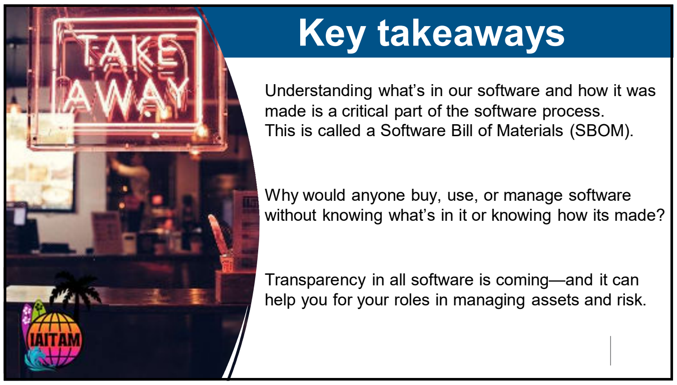
2



Foundational Question

Can you say that you are doing ITAM or SAM if you don't actually know what is in your software?

3



Key takeaways

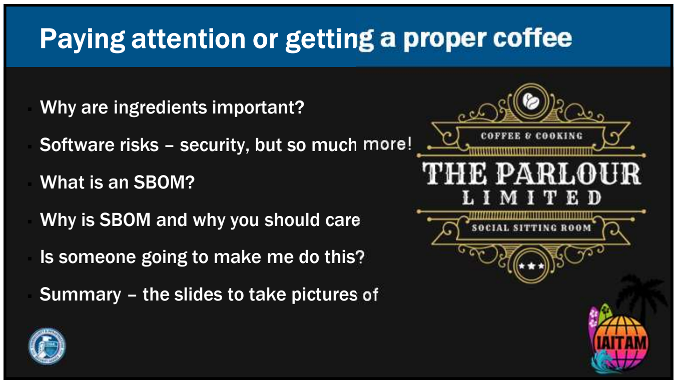
Understanding what's in our software and how it was made is a critical part of the software process. This is called a Software Bill of Materials (SBOM).

Why would anyone buy, use, or manage software without knowing what's in it or knowing how its made?

Transparency in all software is coming—and it can help you for your roles in managing assets and risk.

TAKE AWAY
IAITAM

4

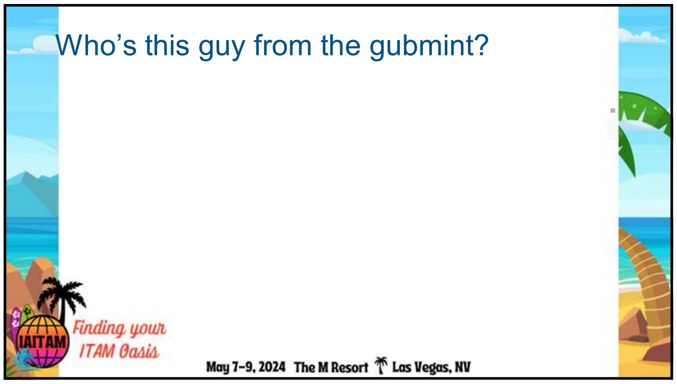


Paying attention or getting a proper coffee

- Why are ingredients important?
- Software risks – security, but so much more!
- What is an SBOM?
- Why is SBOM and why you should care
- Is someone going to make me do this?
- Summary – the slides to take pictures of

COFFEE & COOKING
THE PARLOUR
LIMITED
SOCIAL SITTING ROOM
IAITAM

5

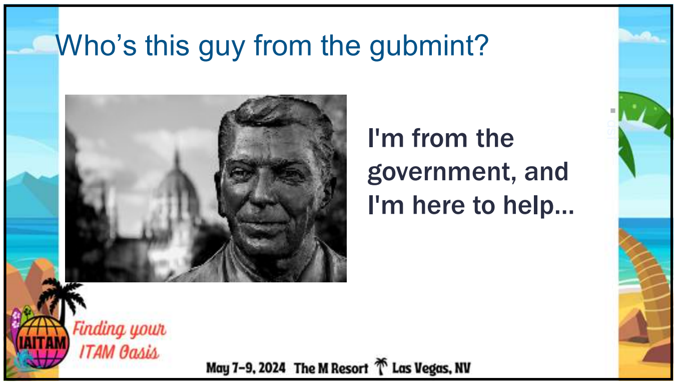


Who's this guy from the gubmint?

Finding your ITAM Oasis

May 7-9, 2024 The M Resort Las Vegas, NV

6



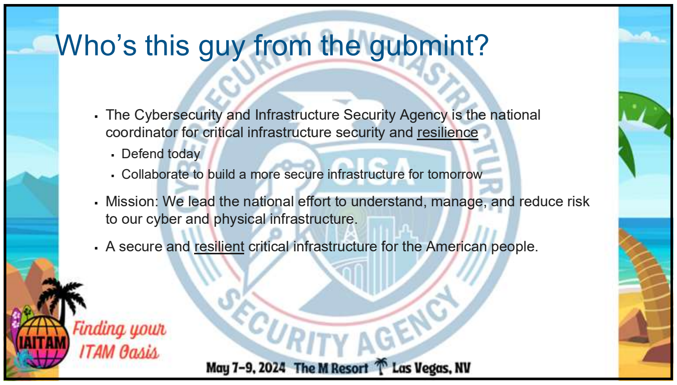
Who’s this guy from the gubmint?

I'm from the government, and I'm here to help…

Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

7



Who’s this guy from the gubmint?

- The Cybersecurity and Infrastructure Security Agency is the national coordinator for critical infrastructure security and resilience
  - Defend today
  - Collaborate to build a more secure infrastructure for tomorrow
- Mission: We lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.
- A secure and resilient critical infrastructure for the American people.

Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

8

An analogy

9

An analogy - Benefits

Hostess
Twinkies
INGREDIENTS: SUGAR, WATER, ENRICHED FLOUR (BLEACHED WHEAT FLOUR, MALTED BARLEY FLOUR, NIACIN, FERROUS SULFATE OR REDUCED IRON, THIAMINE MONONITRATE, RIBOFLAVIN, FOLIC ACID), HIGH FRUCTOSE CORN SYRU TALLOW, EXTROSE, EGG, CONTAINS 2% OR LESS: SOYBEAN OIL, CORN STARCH, MODIFIED CORNSTARCH, HYDROGENATED TALLOW, WHEY, GLYCERIN, SALT, SODIUM ACID PYROPHOSPHATE, BAKING SODA, ENZYMES, SORBIC ACID AND POTASSIUM SORBATE (TO RETAIN FRESHNESS), COTTONSEED OIL, MONO AND DIGLYCERIDES, CELLULOSE GUM, SODIUM STEAROYL LACTYLATE, SOY LECITHIN, XANTHAN GUM, POLYSORBATE 60, MONOCALCIUM PHOSPHATE, NATURAL AND ARTIFICIAL FLAVOR, YELLOW 5, RED 40.
525400
CONTAINS EGG, MILK, SOY, WHEAT
IAITAM

Transparency in food is a critical part of health, lifestyle, and management of our daily life

10

An analogy - Limits

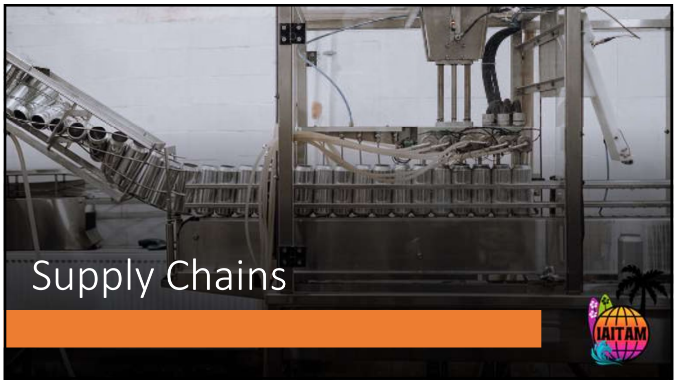
Hostess
Twinkies
INGREDIENTS: SUGAR, WATER, ENRICHED FLOUR (BLEACHED WHEAT FLOUR, MALTED BARLEY FLOUR, NIACIN, FERROUS SULFATE OR REDUCED IRON, THIAMINE MONONITRATE, RIBOFLAVIN, FOLIC ACID), HIGH FRUCTOSE CORN SYRU TALLOW, EXTROSE, EGG, CONTAINS 2% OR LESS: SOYBEAN OIL, CORN STARCH, MODIFIED CORNSTARCH, HYDROGENATED TALLOW, WHEY, GLYCERIN, SALT, SODIUM ACID PYROPHOSPHATE, BAKING SODA, ENZYMES, SORBIC ACID AND POTASSIUM SORBATE (TO RETAIN FRESHNESS), COTTONSEED OIL, MONO AND DIGLYCERIDES, CELLULOSE GUM, SODIUM STEAROYL LACTYLATE, SOY LECITHIN, XANTHAN GUM, POLYSORBATE 60, MONOCALCIUM PHOSPHATE, NATURAL AND ARTIFICIAL FLAVOR, YELLOW 5, RED 40.
525400
CONTAINS EGG, MILK, SOY, WHEAT
IAITAM

This will not *by itself*

- Prevent allergens
- Keep you on a diet
- Enforce dietary rules

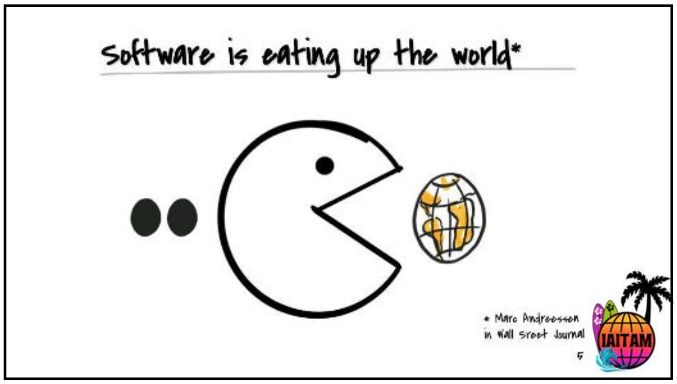
(and you need to know what words mean)

11



Supply Chains

12

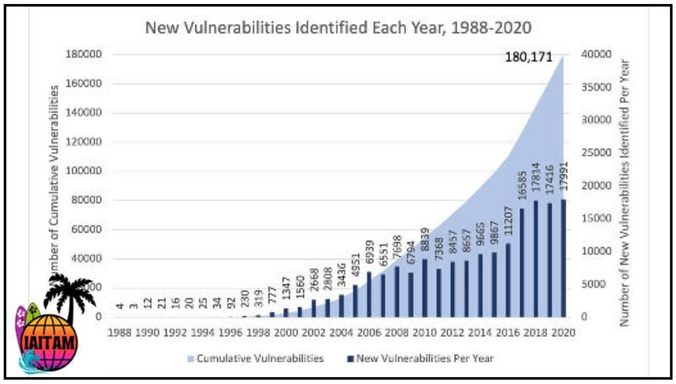


13

Vulnerabilities

“Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.”

14

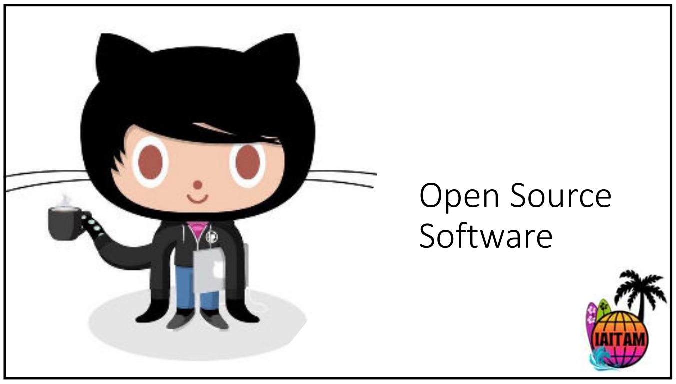


15

Allan…
This isn’t a cybersecurity conference!

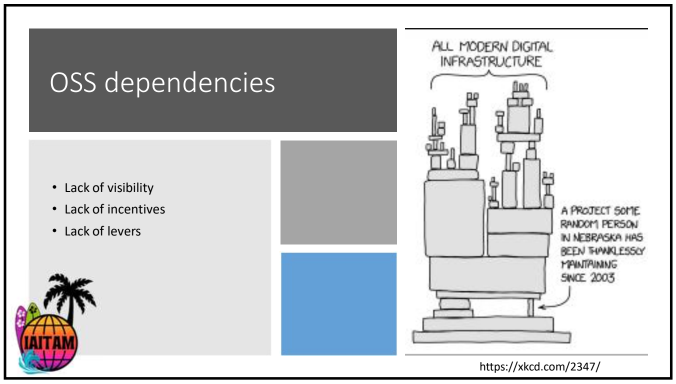
May 7–9, 2024 The M Resort Las Vegas, NV

16



Open Source Software

17



OSS dependencies

- Lack of visibility
- Lack of incentives
- Lack of levers

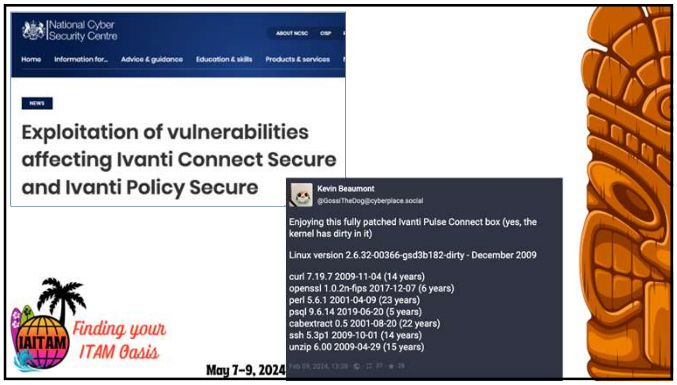
ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003
IAITAM

https://xkcd.com/2347/

18

End of Life and End of Support

19



Exploitation of vulnerabilities affecting Ivanti Connect Secure and Ivanti Policy Secure

Kevin Beaumont
@GossiTheDog@cyberplace.social

Enjoying this fully patched Ivanti Pulse Connect box (yes, the kernel has dirty in it)

Linux version 2.6.32-00366-gsd3b182-dirty - December 2009

```
curl 7.19.7 2009-11-04 (14 years)
openssl 1.0.2n-fips 2017-12-07 (6 years)
perl 5.6.1 2001-04-09 (23 years)
psql 9.6.14 2019-06-20 (5 years)
cabextract 0.5 2001-08-20 (22 years)
ssh 5.3p1 2009-10-01 (14 years)
unzip 6.00 2009-04-29 (15 years)
```

Feb 09, 2024, 13:38

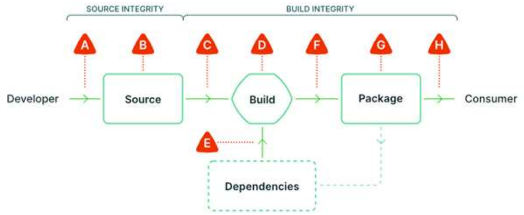
20

Can you guarantee that an asset is current?

FDA
DIB
DEFENSE INDUSTRIAL BASE
CRITICAL INFRASTRUCTURE PROTECTION
SECTOR COORDINATING COUNCIL
CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION
USDA
NIST
PCI DSS COMPLIANT

Patching requirements may be more complex than just single vendors

21



A Submit unauthorized change
B Compromise source repo

C Build from modified source
D Compromise build process
E Use compromised dependency

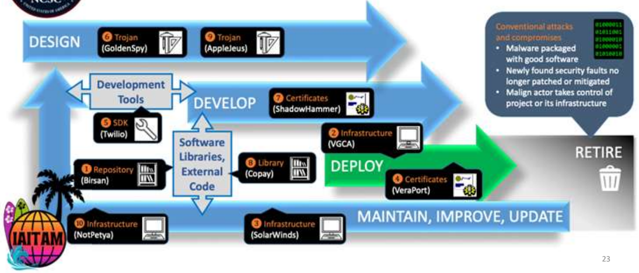
F Upload modified package
G Compromise package repo
H Use compromised package

Source: slsa.dev

22

Software Supply Chain Attacks

Definition: Compromising software through cyber attacks, insider threats, or other malign activities at any stage throughout its entire lifecycle.



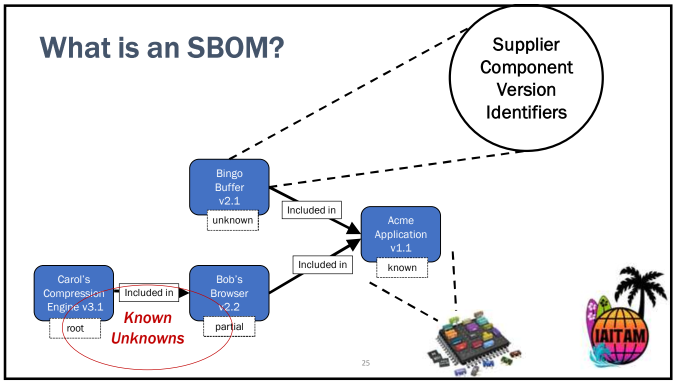
Conventional attacks and compromises
- Malware packaged with good software
- Newly found security faults no longer patched or mitigated
- Malign actor takes control of project or its infrastructure

23

Hidden risks require transparency

24

What is an SBOM?

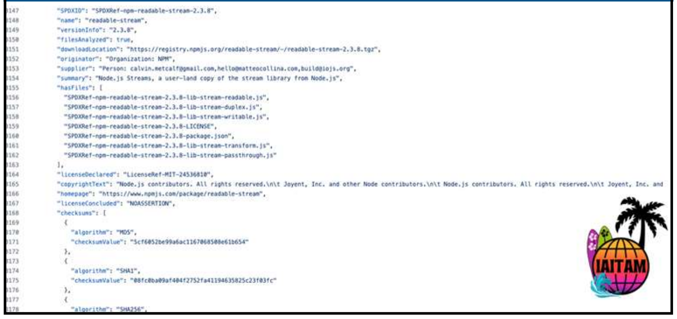


25

An SBOM is a "directed acyclic graph"

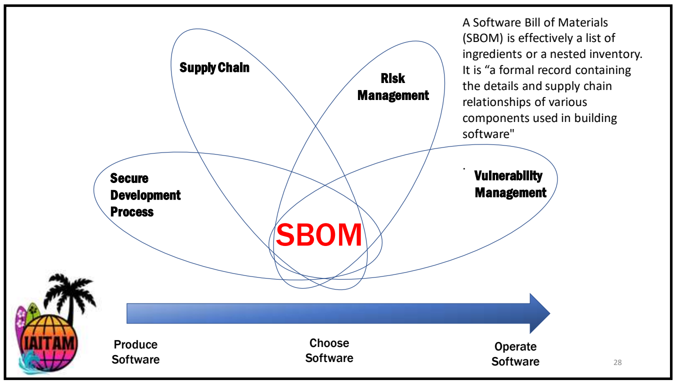
26

An SBOM is just a pile of JSON



```
        "SPDXID": "SPDXRef-npm-readable-stream-2.3.8",
        "name": "readable-stream",
        "versionInfo": "2.3.8",
        "filesAnalyzed": true,
        "downloadLocation": "https://registry.npmjs.org/readable-stream/-/readable-stream-2.3.8.tgz",
        "originator": "Organization: NPM",
        "supplier": "Person: calvin.metcalf@gmail.com,hello@matteocollina.com,build@iojs.org",
        "summary": "Node.js Streams, a user-land copy of the stream library from Node.js",
        "hasFiles": [
          "SPDXRef-npm-readable-stream-2.3.8-lib-stream-readable.js",
          "SPDXRef-npm-readable-stream-2.3.8-lib-stream-duplex.js",
          "SPDXRef-npm-readable-stream-2.3.8-lib-stream-writable.js",
          "SPDXRef-npm-readable-stream-2.3.8-LICENSE",
          "SPDXRef-npm-readable-stream-2.3.8-package.json",
          "SPDXRef-npm-readable-stream-2.3.8-lib-stream-transform.js",
          "SPDXRef-npm-readable-stream-2.3.8-lib-stream-passthrough.js"
        ],
        "licenseDeclared": "LicenseRef-MIT-24536810",
        "copyrightText": "Node.js contributors. All rights reserved.\n\t Joyent, Inc. and other Node contributors.\n\t Node.js contributors. All rights reserved.\n\t Joyent, Inc. and
        "homepage": "https://www.npmjs.com/package/readable-stream",
        "licenseConcluded": "NOASSERTION",
        "checksums": [
          {
            "algorithm": "MD5",
            "checksumValue": "5cf6052be99a6ac1167068508e61b654"
          },
          {
            "algorithm": "SHA1",
            "checksumValue": "08fc0ba09af404f2752fa41194635825c23f03fc"
          },
          {
            "algorithm": "SHA256",
```

27



A Software Bill of Materials (SBOM) is effectively a list of ingredients or a nested inventory. It is “a formal record containing the details and supply chain relationships of various components used in building software"

28

How do we implement this?

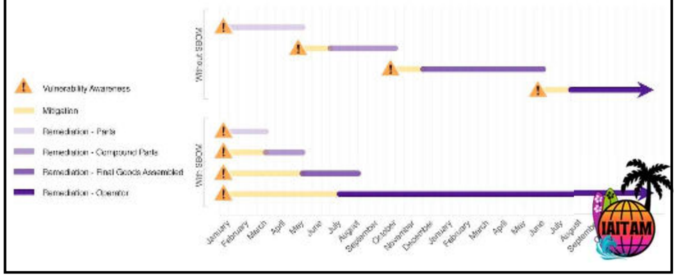
SPDX

CycloneDX

29

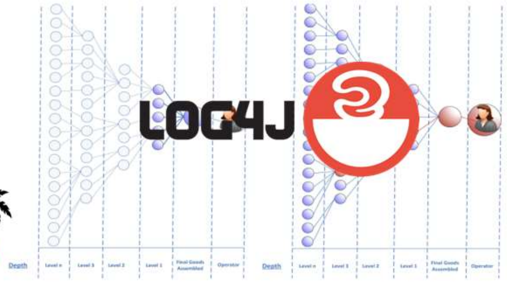
Time to Remediation Case Studies

Without and With SBOM



30

Depth Matters



31

“If we had this today across our organization,
It would save us thousands of hours.”

32

“We like this idea…
We’ll do it when someone makes us.”

- Product Security Lead for F100 company

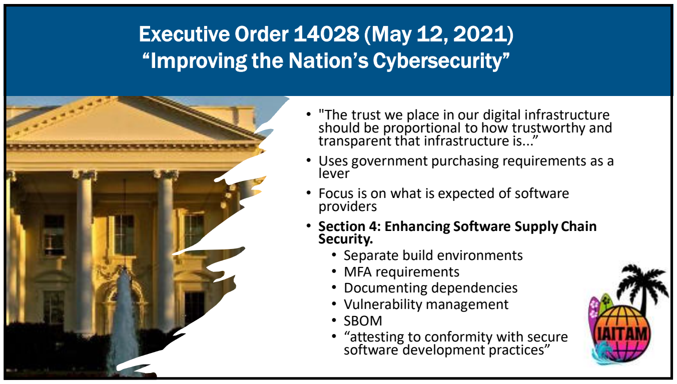
33

The Power of the Purse

&

Compliance

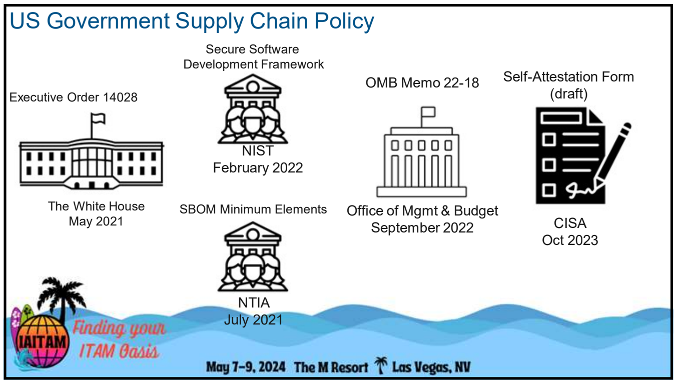
34



Executive Order 14028 (May 12, 2021) "Improving the Nation's Cybersecurity"

- "The trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is..."
- Uses government purchasing requirements as a lever
- Focus is on what is expected of software providers
- **Section 4: Enhancing Software Supply Chain Security.**
  - Separate build environments
  - MFA requirements
  - Documenting dependencies
  - Vulnerability management
  - SBOM
  - "attesting to conformity with secure software development practices"

35



US Government Supply Chain Policy

Executive Order 14028

The White House
May 2021

Secure Software Development Framework

NIST
February 2022

SBOM Minimum Elements

NTIA
July 2021

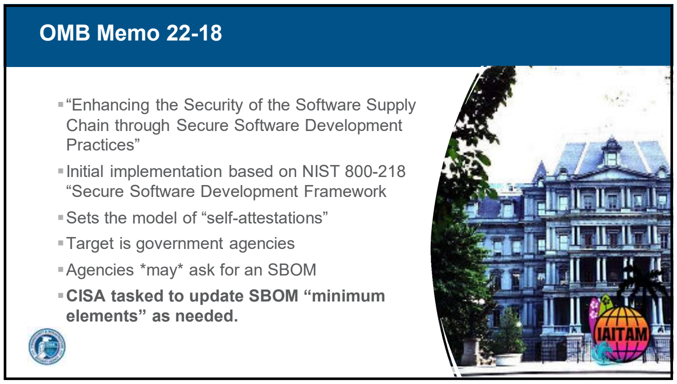
OMB Memo 22-18

Office of Mgmt & Budget
September 2022

Self-Attestation Form (draft)

CISA
Oct 2023

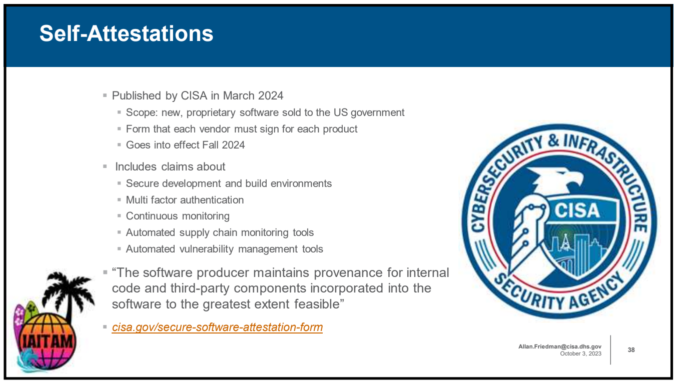
36



OMB Memo 22-18

- “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”
- Initial implementation based on NIST 800-218 “Secure Software Development Framework
- Sets the model of “self-attestations”
- Target is government agencies
- Agencies *may* ask for an SBOM
- **CISA tasked to update SBOM “minimum elements” as needed.**

37



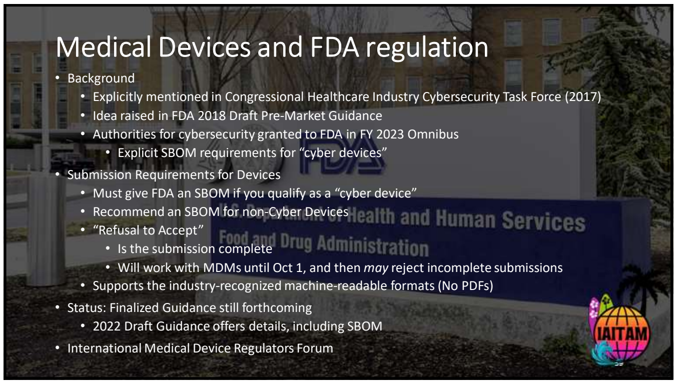
Self-Attestations

- Published by CISA in March 2024
  - Scope: new, proprietary software sold to the US government
  - Form that each vendor must sign for each product
  - Goes into effect Fall 2024
- Includes claims about
  - Secure development and build environments
  - Multi factor authentication
  - Continuous monitoring
  - Automated supply chain monitoring tools
  - Automated vulnerability management tools
- “The software producer maintains provenance for internal code and third-party components incorporated into the software to the greatest extent feasible”
- *cisa.gov/secure-software-attestation-form*

Allan.Friedman@cisa.dhs.gov
October 3, 2023

38

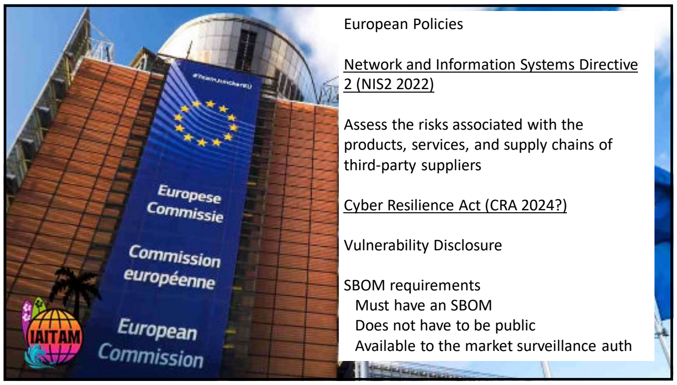
38



Medical Devices and FDA regulation

- Background
  - Explicitly mentioned in Congressional Healthcare Industry Cybersecurity Task Force (2017)
  - Idea raised in FDA 2018 Draft Pre-Market Guidance
  - Authorities for cybersecurity granted to FDA in FY 2023 Omnibus
    - Explicit SBOM requirements for “cyber devices”
- Submission Requirements for Devices
  - Must give FDA an SBOM if you qualify as a “cyber device”
  - Recommend an SBOM for non-Cyber Devices
  - “Refusal to Accept”
    - Is the submission complete
    - Will work with MDMs until Oct 1, and then *may* reject incomplete submissions
  - Supports the industry-recognized machine-readable formats (No PDFs)
- Status: Finalized Guidance still forthcoming
  - 2022 Draft Guidance offers details, including SBOM
- International Medical Device Regulators Forum

39


Europese Commissie
Commission européenne
European Commission
IAITAM

European Policies

Network and Information Systems Directive 2 (NIS2 2022)

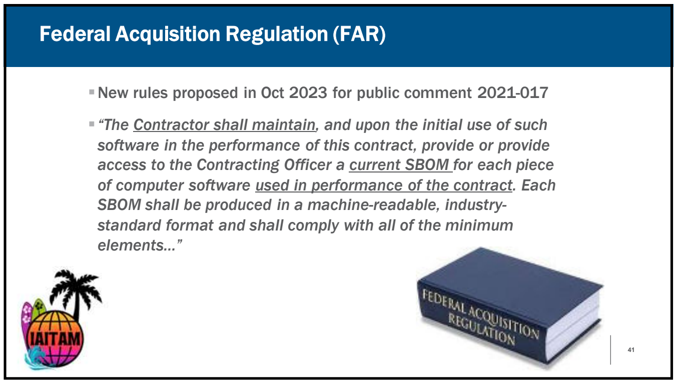
Assess the risks associated with the products, services, and supply chains of third-party suppliers

Cyber Resilience Act (CRA 2024?)

Vulnerability Disclosure

SBOM requirements
- Must have an SBOM
- Does not have to be public
- Available to the market surveillance auth

40


IAITAM
FEDERAL ACQUISITION REGULATION

Federal Acquisition Regulation (FAR)

- New rules proposed in Oct 2023 for public comment 2021-017
- *"The Contractor shall maintain, and upon the initial use of such software in the performance of this contract, provide or provide access to the Contracting Officer a current SBOM for each piece of computer software used in performance of the contract. Each SBOM shall be produced in a machine-readable, industry-standard format and shall comply with all of the minimum elements..."*

41

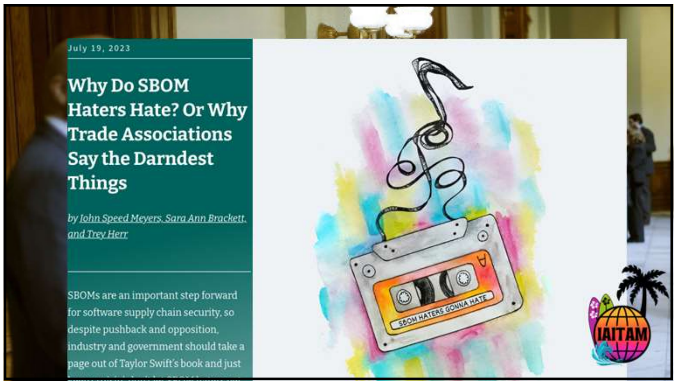
IAITAM
Finding your ITAM Oasis

Red-teaming SBOM
Why not do this?

May 7–9, 2024 The M Resort Las Vegas, NV

42

43


July 19, 2023

Why Do SBOM Haters Hate? Or Why Trade Associations Say the Darndest Things

by John Speed Meyers, Sara Ann Brackett, and Trey Herr

SBOMs are an important step forward for software supply chain security, so despite pushback and opposition, industry and government should take a page out of Taylor Swift's book and just

44

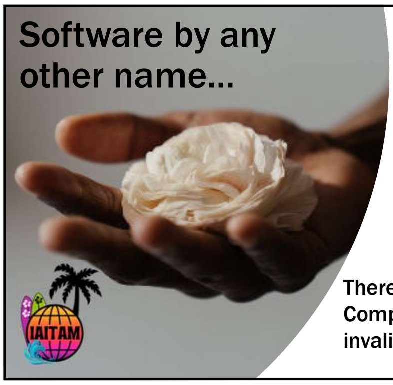
- "Roadmap to the attackers"
- Intellectual Property
- Do we actually need it?
- It's just not ready…

Red-teaming SBOM
Why not do this?

45

Software by any other name…

46



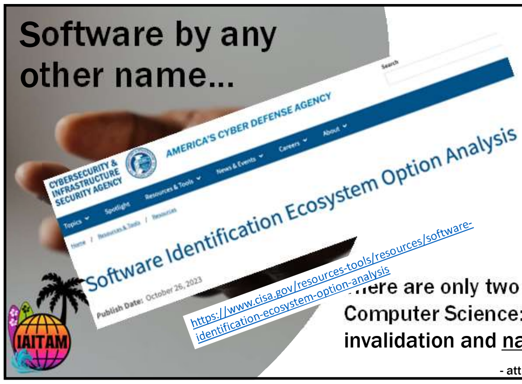
There are only two hard things in Computer Science: cache invalidation and naming things.”

- attributed to Phil Karlton

46

Software by any other name…

47



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics ⌄ Spotlight Resources & Tools ⌄ News & Events ⌄ Careers ⌄ About ⌄

Home / Resources & Tools / Resources

Software Identification Ecosystem Option Analysis

Publish Date: October 26, 2023

https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis

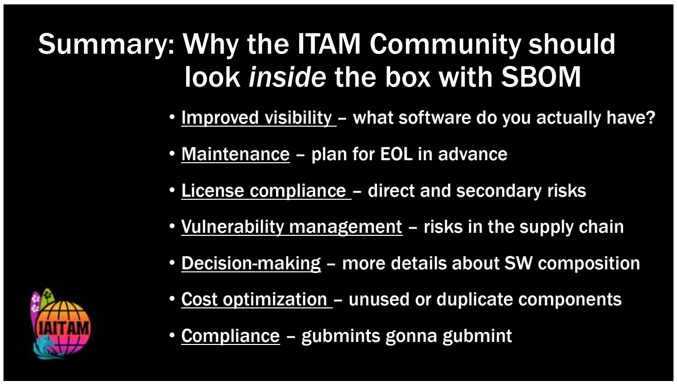
here are only two hard things in Computer Science: cache invalidation and naming things.”

- attributed to Phil Karlton

47

Hardware Bill of materials

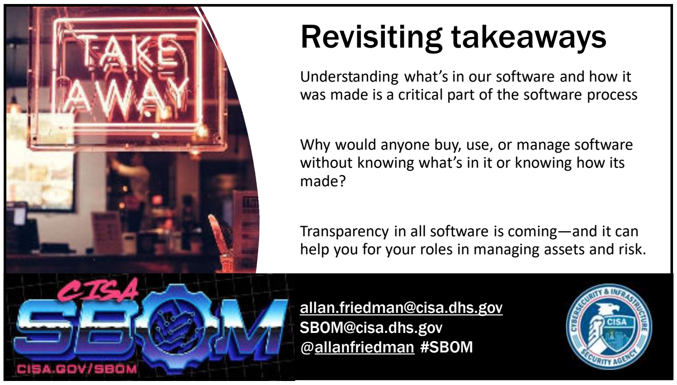
48



Summary: Why the ITAM Community should look *inside* the box with SBOM

- Improved visibility – what software do you actually have?
- Maintenance – plan for EOL in advance
- License compliance – direct and secondary risks
- Vulnerability management – risks in the supply chain
- Decision-making – more details about SW composition
- Cost optimization – unused or duplicate components
- Compliance – gubmints gonna gubmint

49



Revisiting takeaways

Understanding what's in our software and how it was made is a critical part of the software process

Why would anyone buy, use, or manage software without knowing what's in it or knowing how its made?

Transparency in all software is coming—and it can help you for your roles in managing assets and risk.

allan.friedman@cisa.dhs.gov
SBOM@cisa.dhs.gov
@allanfriedman #SBOM

50

IAITAM ACE
May 7–9, 2024 The M Resort Las Vegas, NV
IAITAM
Finding your IAITAM Oasis

CISA.gov/SBOM
SBOM@cisa.dhs.gov

allan.friedman@cisa.dhs.gov

51