

SECURING THE CHAIN: LEVERAGING SBOMS IN FEDERAL ACQUISITIONS TO ENHANCE OPEN SOURCE SOFTWARE INTEGRITY

KAMMY MANN
CYBERSECURITY DIVISION
OFFICE OF THE TECHNICAL DIRECTOR
SEPTEMBER 17, 2024

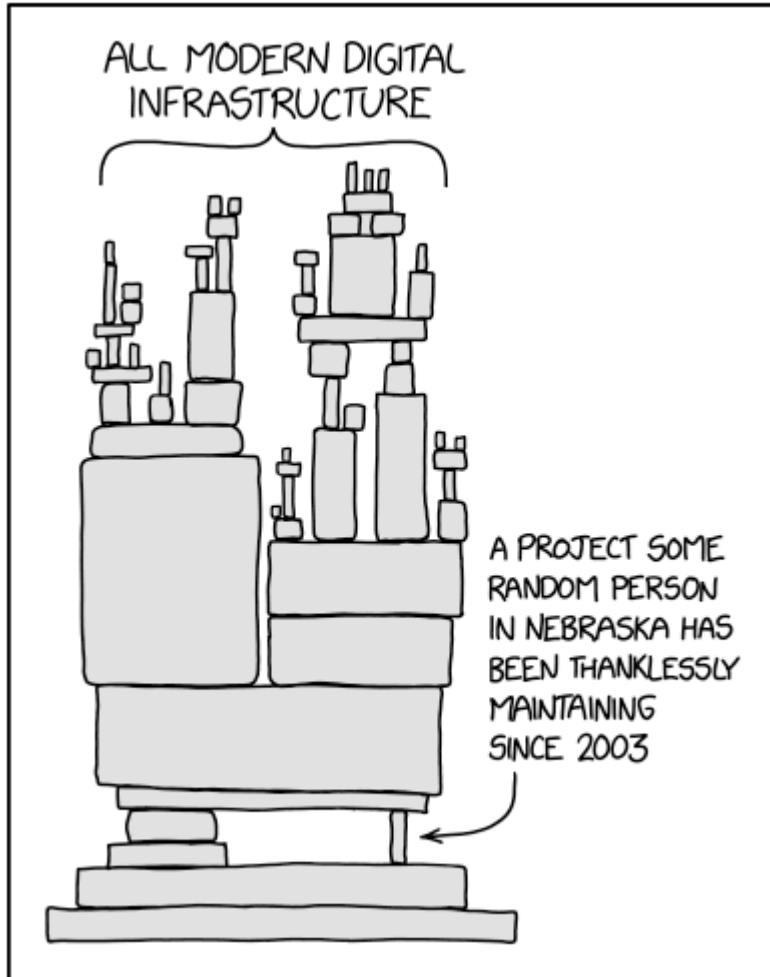


Agenda

- What is Open Source Software (OSS)?
- Vulnerabilities in OSS
- What are SBOMs?
- SBOMs for Risk Reduction
- What is the DHS S&T SVIP?
- Outputs of DHS S&T SVIP R&D Project
- CISA Secure by Design Initiative
- How can the Federal Acquisition Community Secure Software Supply Chain?
- Resources



What is Open Source Software (OSS)?



<https://xkcd.com/2347/>

“Software for which the human-readable source code is available for use, study, re-use, modification, enhancement, and re-distribution by the users of such software” – [Public Law 115-232](#)

Open Source Software has generated over **\$8T** in value to our global society*

*Hoffmann, Manuel, Frank Nagle, and Yanuo Zhou. "[The Value of Open Source Software.](#)" Harvard Business School Working Paper, No. 24-038, January 2024.

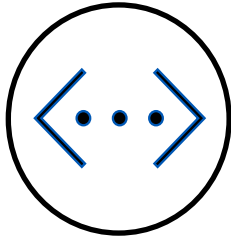


Benefits of OSS in Government

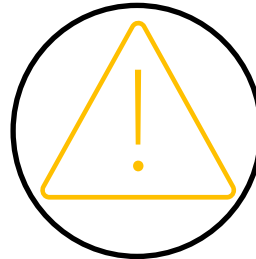
- The public funds government projects – the public should use what it has paid for.
- Collaboration easier among agencies, contractors and the public.
- Reduces the risk of future vendor lock-in.
- Allows critical evaluation of software and participating from others.
- Levels the playing field for future procurements and increases competition.
- Shows the developer's skills.



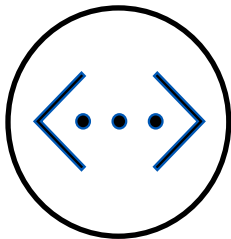
Vulnerabilities in OSS



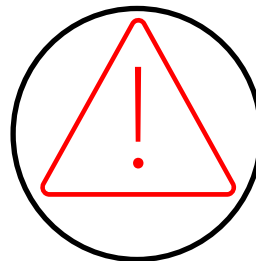
96%
of the total
codebases scanned
contained
open source



84%
of codebases assessed for risk
contained at least one open source **vulnerability**.



77%
of all code in the
total code bases scanned
originated from
open source



74%
of codebases assessed for risk
contained **high risk vulnerabilities**.

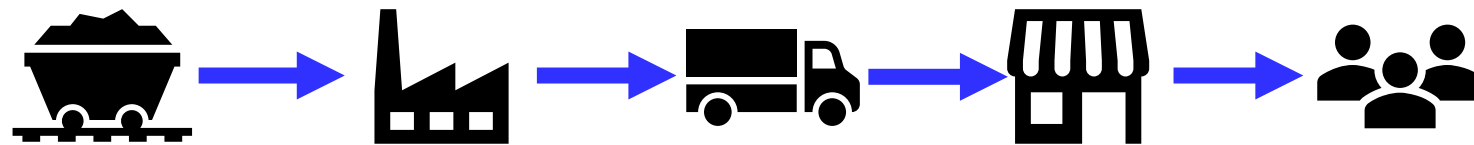
The report* highlights the pervasiveness of OSS and the dangers of not properly managing it



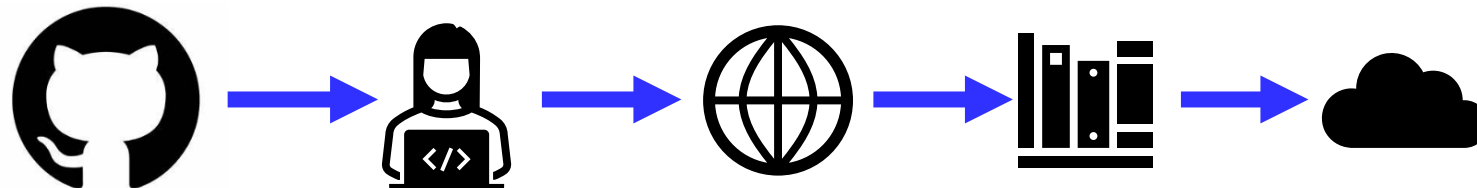
[*Synopsys 2024 Open Source Security and Risk Analysis Report](#)

Software Supply Chain

Traditional
Supply
Chain



Software
Supply
Chain



Ubiquity of OSS means vulnerabilities have widespread downstream consequences in the supply chain

The Case

Are Twinkies Vegan? Can Vegans Eat Twinkies?

- Food ingredients
- Safety Data Sheet
- Hardware Bills of

By: Daniel B. • Date: December 29, 2022 • Time to read: 5 min.



Would you feed
didn't

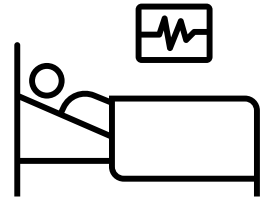
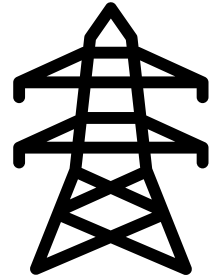
Answer: No. The presence of beef fat and egg makes them unsuitable for vegans.



Are Twinkies Vegan? Can Vegans Eat Twinkies?



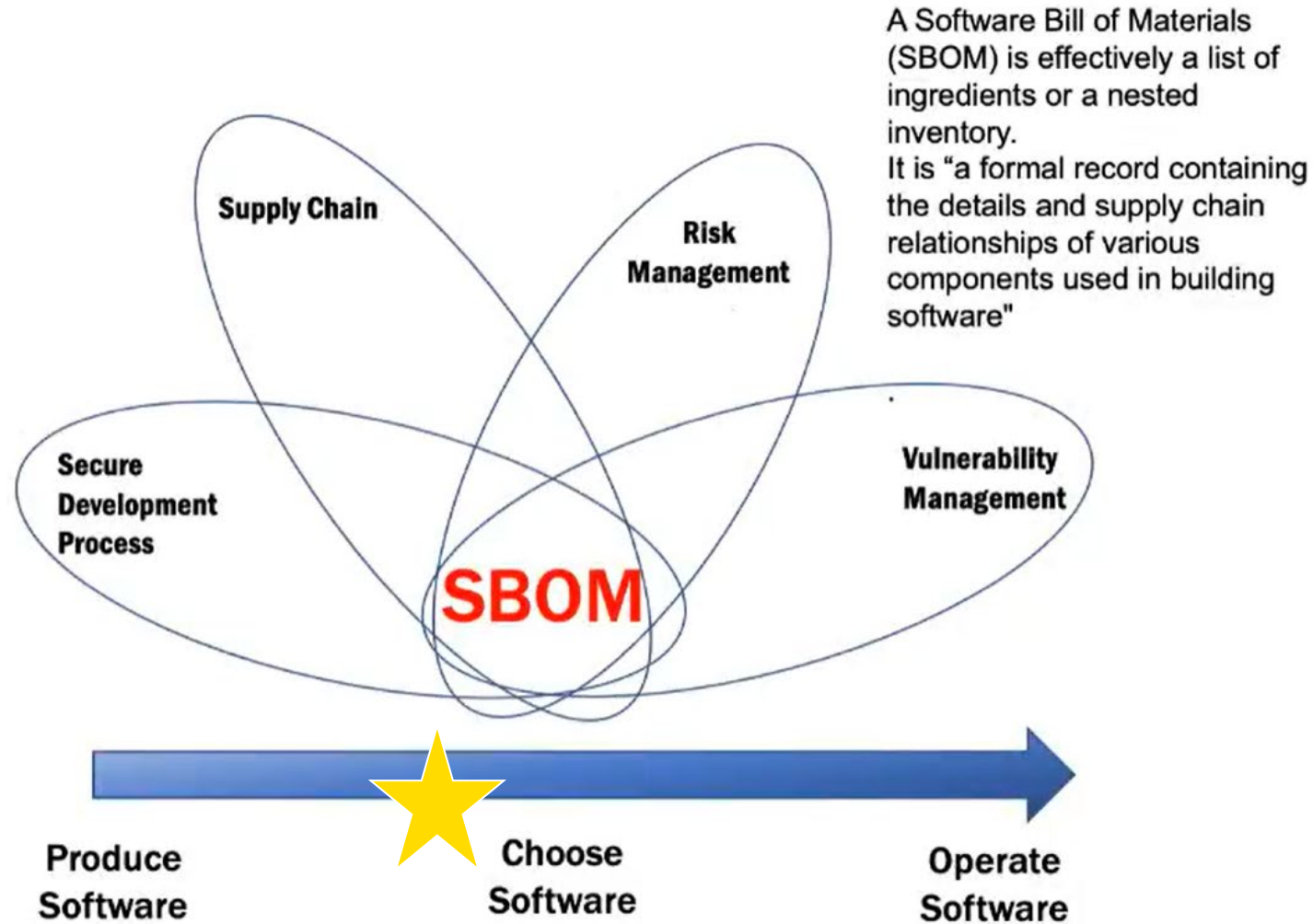
“Know what you have”



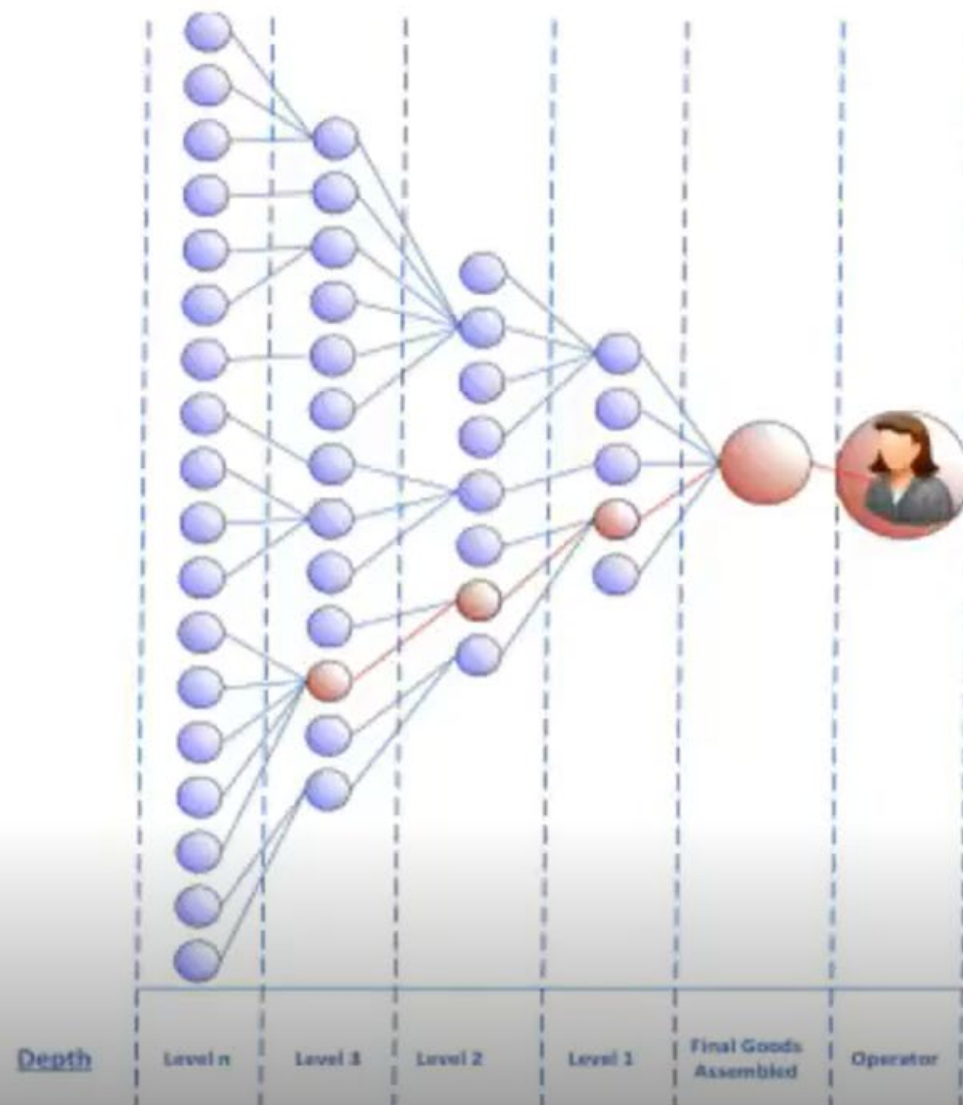
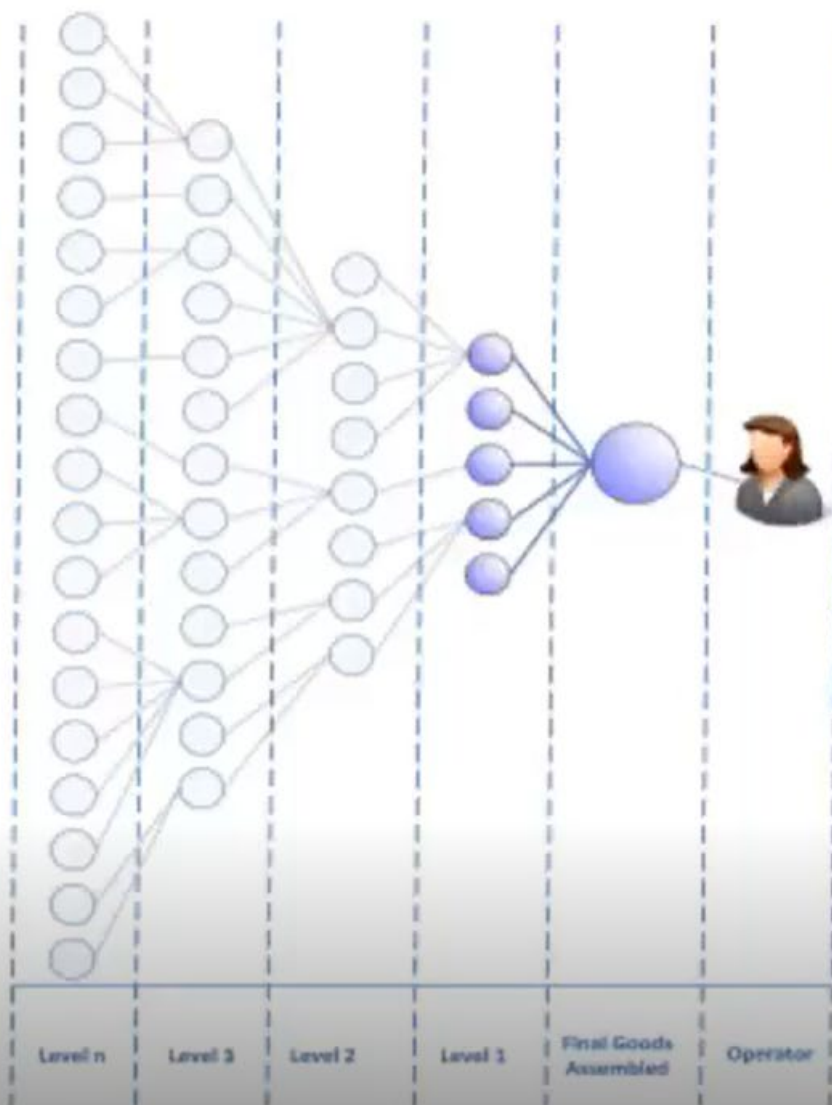
LOG4J



SBOM in the Software Lifecycle

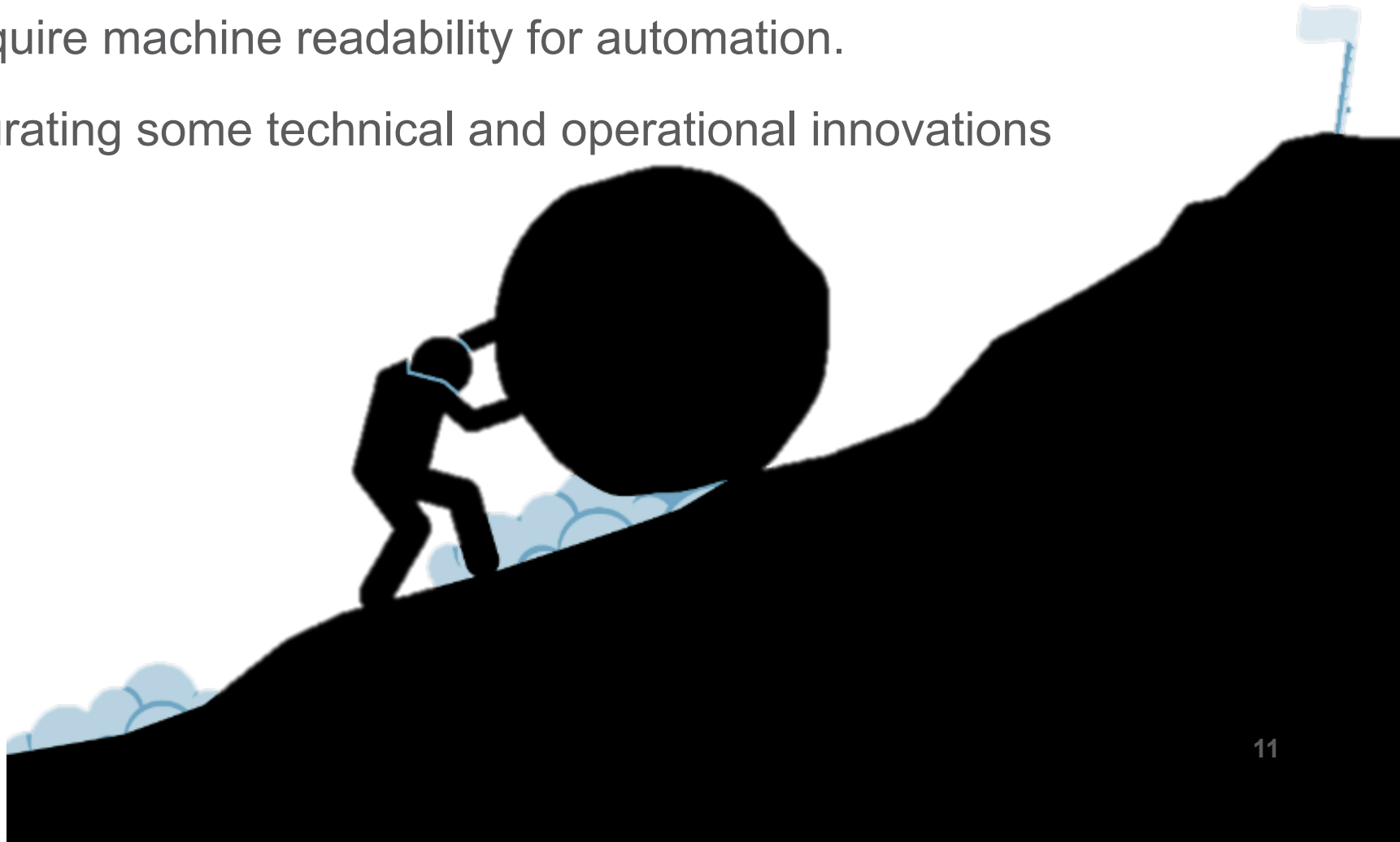


Depth Matters



Why aren't we doing this today?

- Licensing concerns and open source restrictions
- It's hard: many benefits require machine readability for automation.
- It's complex: involved integrating some technical and operational innovations



Current Proof of Concepts



Medical



Automotive



Electrical Grid



Executive Order 14028



MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

 BRIEFING ROOM  PRESIDENTIAL ACTIONS



[Executive Order on Improving the Nation's Cybersecurity | The White House](#)

- “The trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is...”
- The EO defines SBOM and identifies the value proposition in 10(j)
- Section 4: Enhancing Software Supply Chain Security
 - 4(f) – NTIA defines the “minimum elements” of SBOM
 - 4(e)(vii) – Commerce and USG defines guidance on “providing a purchaser a Software Bill of Materials (SBOM) for each product”
 - 4(k) and 4(n) – guidance on specific implementations

SPDX vs. CycloneDX



SPDX



CycloneDX



Two SBOM Data Standards within the
Open Source Community





SILICON VALLEY INNOVATION PROGRAM

SVIP reaches out to innovation communities across the nation and the world to harness commercial R&D for government applications, co-invest in, and accelerate the transition of technology to the commercial market.

GOALS

- Develop and adapt commercial technologies for deployment to DHS Operational Components to meet DHS needs
- Promote economic development through startup/small business growth



EDUCATE

Help investors and entrepreneurs understand DHS's hard problems



FUND

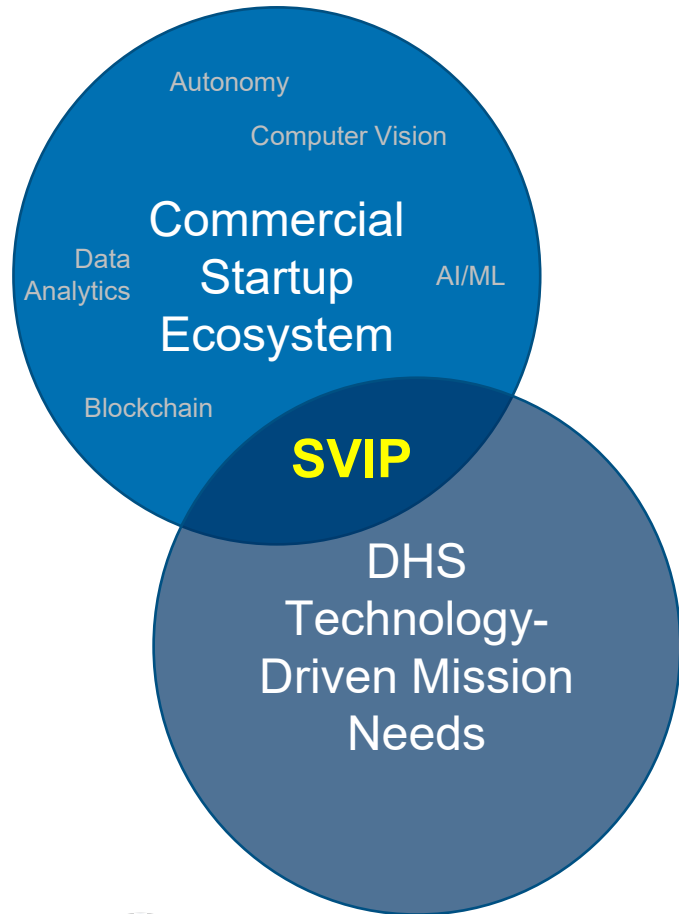
Provide accelerated non-dilutive funding (up to \$2M US) for product development to address DHS's needs



TEST

Provide test environments and opportunities for operational evaluation

DHS S&T Silicon Valley Innovation Program (SVIP)



Up to \$2M over 24 months
\$50-500K/phase over 4 Phases

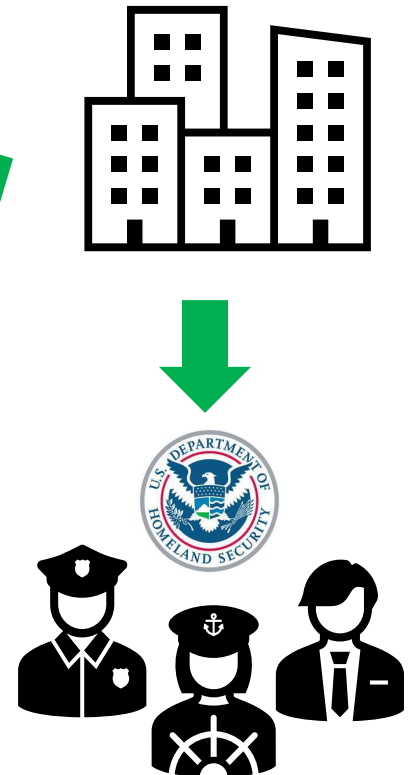


Other Transaction Authority awards to non-traditional companies (U.S. and international)



Products Shaped with DHS Needs

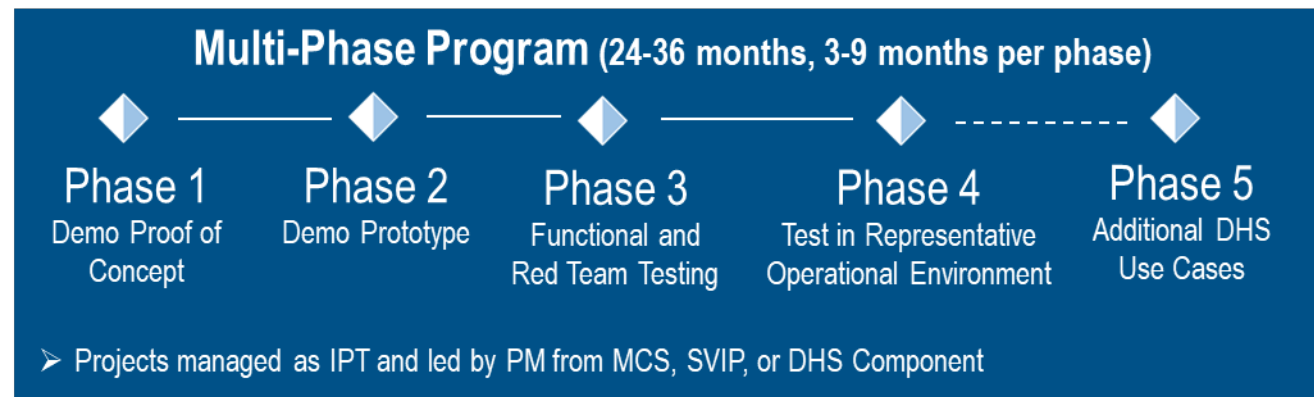
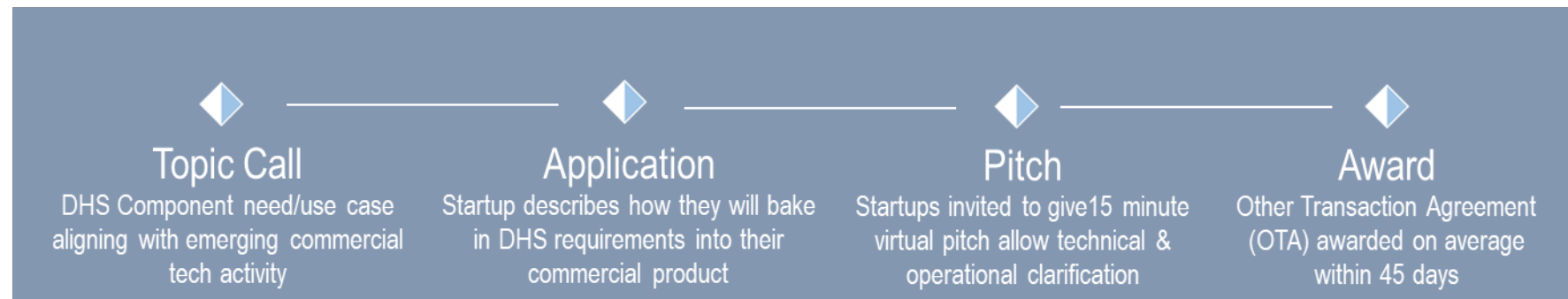
Commercialization



Acquisition Process

Simplify Competition and Contracting Process

- Umbrella Other Transaction Solicitation (OTS) allows topic calls to be issued without additional acquisition plans
- Standardize contracting template including Terms & Conditions across awards
- Flexibility for additional DHS Components with common requirements to participate



- ❑ OTAs awarded per phase
- ❑ Multiple awards, approaches de-risk startup solutions
- ❑ Fixed-Price, Milestones-based payments
- ❑ Solutions transitioned to commercial market



Open Global Solicitation in 2022

News Release: DHS S&T Forms New Startup Cohort to Strengthen Software Supply Chain Visibility Tools

Release Date: April 27, 2023

FOR IMMEDIATE RELEASE

[S&T Public Affairs](#) ☎, 202-254-2385

WASHINGTON - The Department of Homeland Security (DHS) [Science and Technology Directorate](#) (S&T) announced seven awardees from the “[Software Supply Chain Visibility Tools](#)” topic call which sought innovative technologies to provide software bill of materials (SBOMs) based capabilities for stakeholders within the enterprise, system administrator, and software development communities. S&T’s [Silicon Valley Innovation Program](#) (SVIP) issued the solicitation, seeking open-source-based technical solutions to provide the transparency to form the foundation for a high-assurance software supply chain, and to enable visibility into software supply chains and new risk assessment capabilities that serve the mission needs of DHS components and programs, including the Cybersecurity and Infrastructure Security Agency (CISA).

“To defend against the increasing number of software attacks, it’s critical to utilize innovative tools that create a more transparent software supply chain,” said Melissa Oh, SVIP Managing Director. “DHS is tapping into the startup community to develop technology that will shine a light on risks within supply chains and bolster the overall cybersecurity of organizations.”

The seven awardees will work as a cohort to develop two core software modules—a multi-format SBOM translator and a software component identifier translator—to be delivered as open-source libraries which, in turn, will be integrated with their SBOM enabled commercial products.

“Vulnerabilities in software are a key risk in cybersecurity, with known exploits being a primary path for bad actors to inflict a range of harms. By leveraging SBOMs as key elements of software security, we can mitigate the risk to the software supply chain and respond to new risks faster, and more efficiently,” said Allan Friedman, CISA Senior Advisor and Strategist. “A thriving ecosystem for SBOM tools and solutions will be key to shaping a more transparent software-driven world.”

S&T awarded Phase 1 Other Transaction Awards to seven companies: AppCensus, Inc., Chainguard, Inc., Deepbits Technology, Inc., Manifest Cyber, Inc., Scribe Security, TestifySec, LLC, and Veramine, Inc. Through a competitive process, these awardees presented innovative solutions that have the potential to provide immediate impacts to the cybersecurity market:



[S&T Forms New Startup Cohort to Strengthen Software Supply Chain Visibility Tools | Homeland Security \(dhs.gov\)](#)



SOFTWARE SUPPLY CHAIN VISIBILITY TOOLS

Other Transaction Solicitation Call # 70RSAT22R00000027

SBOM
Generation

- AppCensus
- Chainguard
- Deepbits
- Manifest
- Scribe
- TestifySec
- Verimine

SIEM
Plug-In

- Manifest
- TestifySec

Multi-Format SBOM
Translator
---- Open Source ----
Software
Component
Identifier Translator

Visualization

- AppCensus
- Manifest
- Scribe
- TestifySec

IDE
Plug-In



Science &
Technology

Phase 1 – Success!

Open Source

Can Protobom end the SBOM format wars?

Adolfo García Veytia, Staff OSS Engineer and John Speed Meyers, Principal Research Scientist

July 31, 2023



TL;DR Tired of fretting about SBOM formats rather than focusing on software supply chain security? A new open source tool, 'protobom,' frees you of this burden, help and your organization create and consume SBOMs regardless of SBOM format.




← Post

 **Tracy Miranda**
@tracymiranda

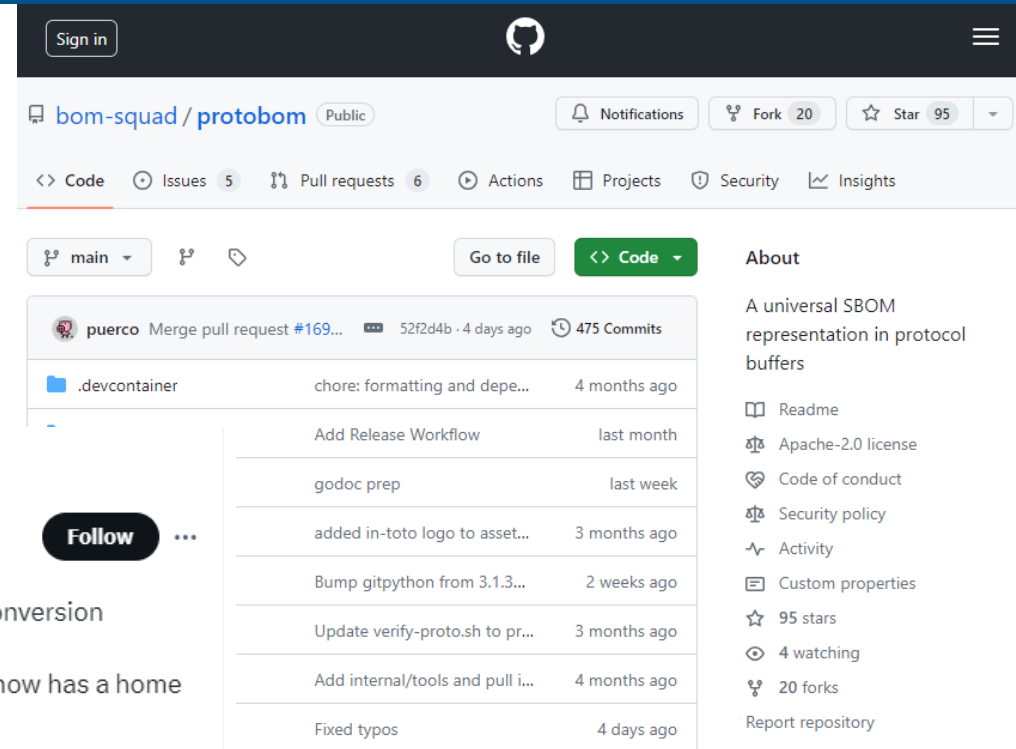
Protobom is key to SBOM interoperability by allowing conversion between SPDX & CycloneDX. It is a startup collaboration, funded by the US govt and now has a home in the vendor-neutral [@openssf](#)!

Congratulations [@puerco](#) on your leadership with this game-changing SBOM project.

 **puerco** @puerco · Jan 9
I'm incredibly proud to share that the protobom project we've been building together with @dhsscitech to solve #SBOM I/O was accepted to the @openssf sandbox 🎉🎉🎉

Congrats @AppCensusInc @chainguard_dev @deepbits_tech @manifestcyber...
[Show more](#)

12:55 PM · Jan 9, 2024 · 535 Views



Sign in

bom-squad / protobom Public

Notifications Fork 20 Star 95

Code Issues 5 Pull requests 6 Actions Projects Security Insights

main

Go to file Code

puerco Merge pull request #169... 52f2d4b · 4 days ago 475 Commits

.devcontainer	chore: formatting and depe...	4 months ago
	Add Release Workflow	last month
	godoc prep	last week
	added in-toto logo to asset...	3 months ago
	Bump gitpython from 3.1.3...	2 weeks ago
	Update verify-proto.sh to pr...	3 months ago
	Add internal/tools and pull i...	4 months ago
	Fixed typos	4 days ago

About

A universal SBOM representation in protocol buffers

- Readme
- Apache-2.0 license
- Code of conduct
- Security policy
- Activity
- Custom properties
- 95 stars
- 4 watching
- 20 forks

Report repository

Press Release

CISA, DHS S&T and OpenSSF Announce Global Launch of Software Supply Chain Open Source Project

April 16, 2024 | Press Release



Protobom project allows for easy creation and translation of Software Bill of Materials (SBOMs)



Cybersecurity and Infrastruc...

480,546 followers

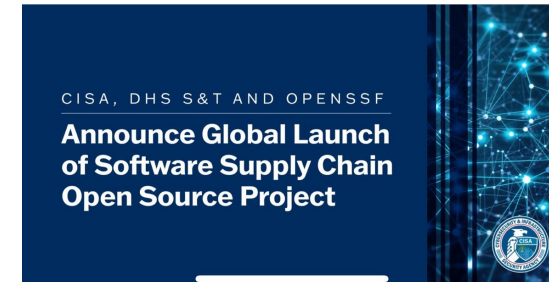
1w · Edited ·

In collaboration with the Open Source Security Foundation (OpenSSF) and the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), we announced the launch and availability of Protobom, a new and innovative open source software supply chain tool. It enables all organizations, including system administrators and software development communities, to read and generate SBOMs and file data, as well as translate this data across standard industry SBOM formats.

Protobom is a step towards greater efficiency and interoperability by translating across the widely used formats, so that tools and organizations can focus on what's important. It is a positive solution that helps shape a more transparent software-driven world which will encourage more organizations to adopt the use of SBOM.

The OpenSSF has further committed to facilitating the open source and collaborative development of Protobom while encouraging the growth of an open source contributor community.

<https://lnkd.in/g5f4PcrC>



[CISA, DHS S&T and OpenSSF Announce Global Launch of Software Supply Chain Open Source Project – Open Source Security Foundation](#)

SVIP Expectations

- Open-source license ensures that the software is patent free, royalty free, non-discriminatory, available to all and free to implement on a global basis for both closed source and open source
- Open-source libraries will be delivered with SBOMs
- Commercial products (Digital Wallets and Mobile Verifiers) encouraged to be delivered with SBOMs
 - All awarded companies have confirmed their intention to deliver SBOMs with their commercial products



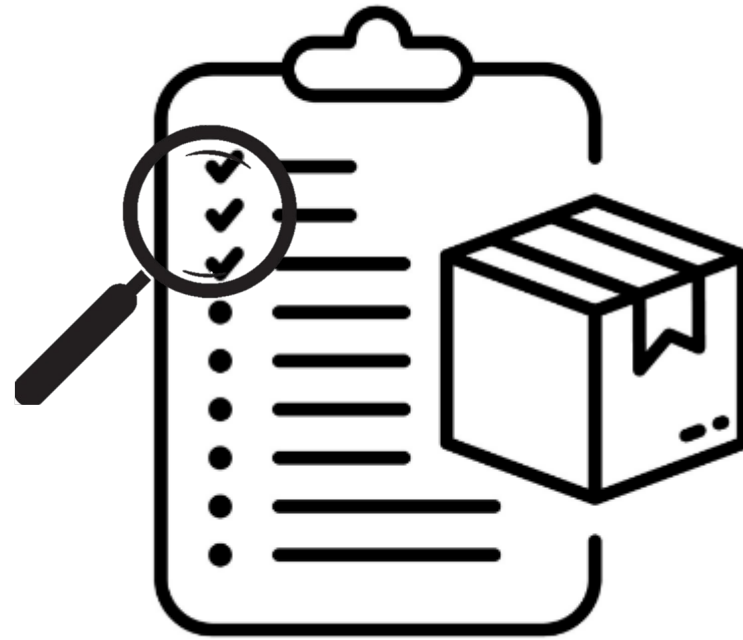
Software Security Requirements

- SHOULD provide a Software Bill of Materials (SBOM) containing the details and supply chain relationships of various components used in building your software
 - SHALL contain the minimum elements for a SBOM as defined in the joint report by the Department of Commerce and the National Telecommunications and Information Administration
 - <https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom>



SBOM: Part of a complete security toolkit

Asset
Management



SBOM

Secure
Development

Risk
Management

Vulnerability
Management



SBOM isn't a "silver bullet" but part of an organization's cybersecurity posture

CISA Secure by Design



- “Secure-by-Design” means that technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure.
- Software Product Security Principles:
 1. The burden of security should not fall solely on the customer.
 2. Embrace radical transparency and accountability.
 3. Build organizational structure and leadership to achieve these goals.

SBOM is a key Secure-by-Design Tactic



Call to Action/Take Aways

- Promote Open Source Software and the OSS community!
 - Responsible consumption, sustainable contribution
- When doing a Federal Acquisition of software **ASK FOR A SBOM**
- Further research on using SBOMs in the cost estimation process
- Drink our own champagne – SVIP asking for SBOMs for all delivered software AND in contract language (even before FAR requirements)
- Leverage the start-up ecosystem, look for creative ways to solve sticky problems
- Require software manufacturers to build safety into their products vs. onus on consumer.



Additional Resources (DHS/CISA)

- [SVIP & CISA: Enhancing Software Security with SBOMs \(youtube.com\)](#)
- [Software Bill of Materials \(SBOM\) | CISA](#)
- [Secure by Design | CISA](#)
- [Open Source Software Security | CISA](#)
- [SVIP | Homeland Security \(dhs.gov\)](#)
- [S&T Forms New Startup Cohort to Strengthen Software Supply Chain Visibility Tools | Homeland Security \(dhs.gov\)](#)
- [CISA, DHS S&T and OpenSSF Announce Global Launch of Software Supply Chain Open Source Project – Open Source Security Foundation](#)
- [Protobom – Open Source Security Foundation \(openssf.org\)](#)



Other Resources

- [Open Source Software FAQ \(defense.gov\)](#)
- [Planning | 18F De-risking Guide](#)
- [Four key principles for effective custom software development | 18F De-risking Guide](#)
- [Best practices for open source software security | 18F De-risking Guide](#)
- [Software Security in Supply Chains: Software Bill of Materials \(SBOM\) | NIST](#)
- https://ntia.gov/sites/default/files/publications/ntia_sbom_framing_2nd_edition_2021102_1_0.pdf
- https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov20_19.pdf
- <https://www.fda.gov/media/119933/download>
- [Synopsys 2024 Open Source Security and Risk Analysis Report](#)
- Hoffmann, Manuel, Frank Nagle, and Yanuo Zhou. "[The Value of Open Source Software.](#)" Harvard Business School Working Paper, No. 24-038, January 2024.
- [Executive Order on Improving the Nation's Cybersecurity | The White House](#)





Questions?

Contact information:

Katharine.Mann@cisa.dhs.gov

Also:

www.cisa.gov/sbom

