SBOM'S AND STARTUPS

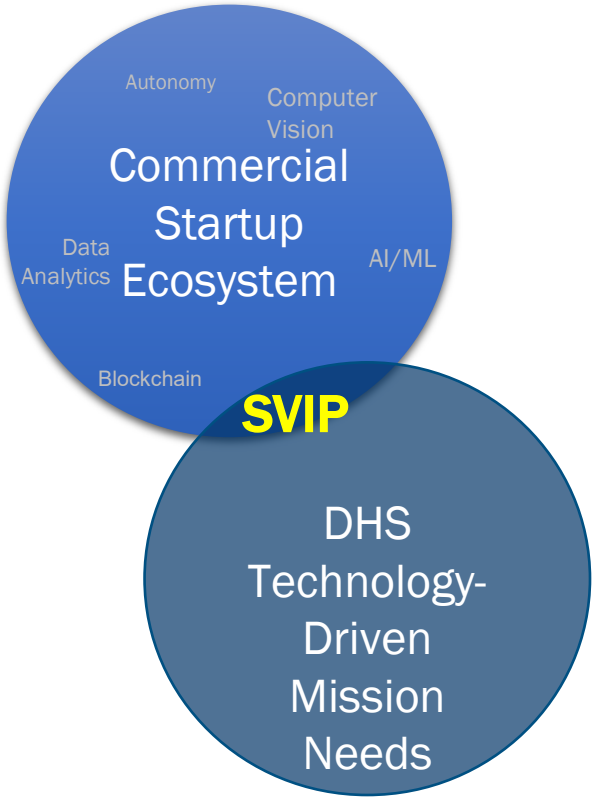
MAKING INVESTMENTS TO ENCOURAGE THE ECOSYSTEM

KAMMY MANN
CYBERSECURITY DIVISION (CSD)
OFFICE OF THE TECHNICAL DIRECTOR (OTD)
FEBRUARY 29, 2024

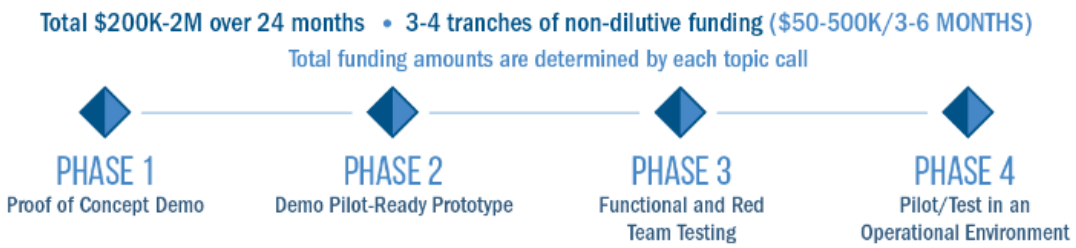
Agenda

- What is SVIP?
- How is DHS helping to seed the ecosystem with SBOM tooling?
- How is DHS encouraging the development of SBOMs in the solutions we are funding?
- Guidance language in solicitations
- Q&A

What is the Silicon Valley Innovation Program (SVIP)?



- Founded in 2015 within DHS S&T to…
  - Accelerate the transition of innovative commercial technology to operational use
  - Shape the product roadmaps of early-stage commercial startups to bake DHS requirements into their solutions as they hit the open market
- How? By providing up to $800K-$2M per startup over 24 months
- Not a typical R&D program
  - Products must have a commercial path and be production-ready in 24 months



Phase 5: May be awarded if the government determines that further operational testing is required, and/or the technology is applicable in additional DHS use cases. Phase 5 Other Transactional Agreements will be scaled to fit the cost and length of time for the mission need/requirement and are not restricted by Phases 1–4.

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."

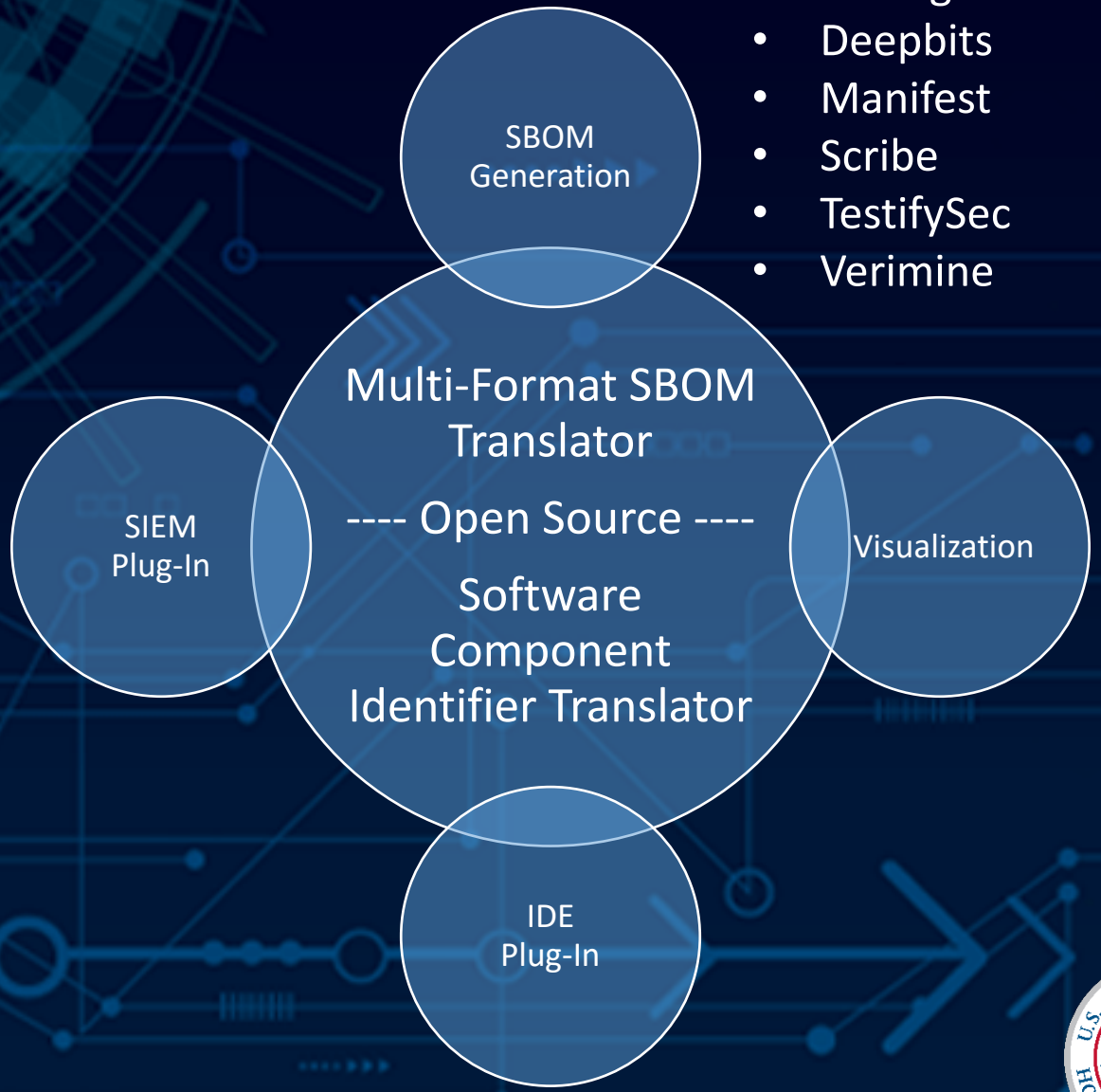
The seven awardees will work as a cohort to develop two core software modules—a multi-format SBOM translator and a software component identifier translator—to be delivered as open-source libraries which, in turn, will be integrated with their SBOM enabled commercial products.

"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)

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



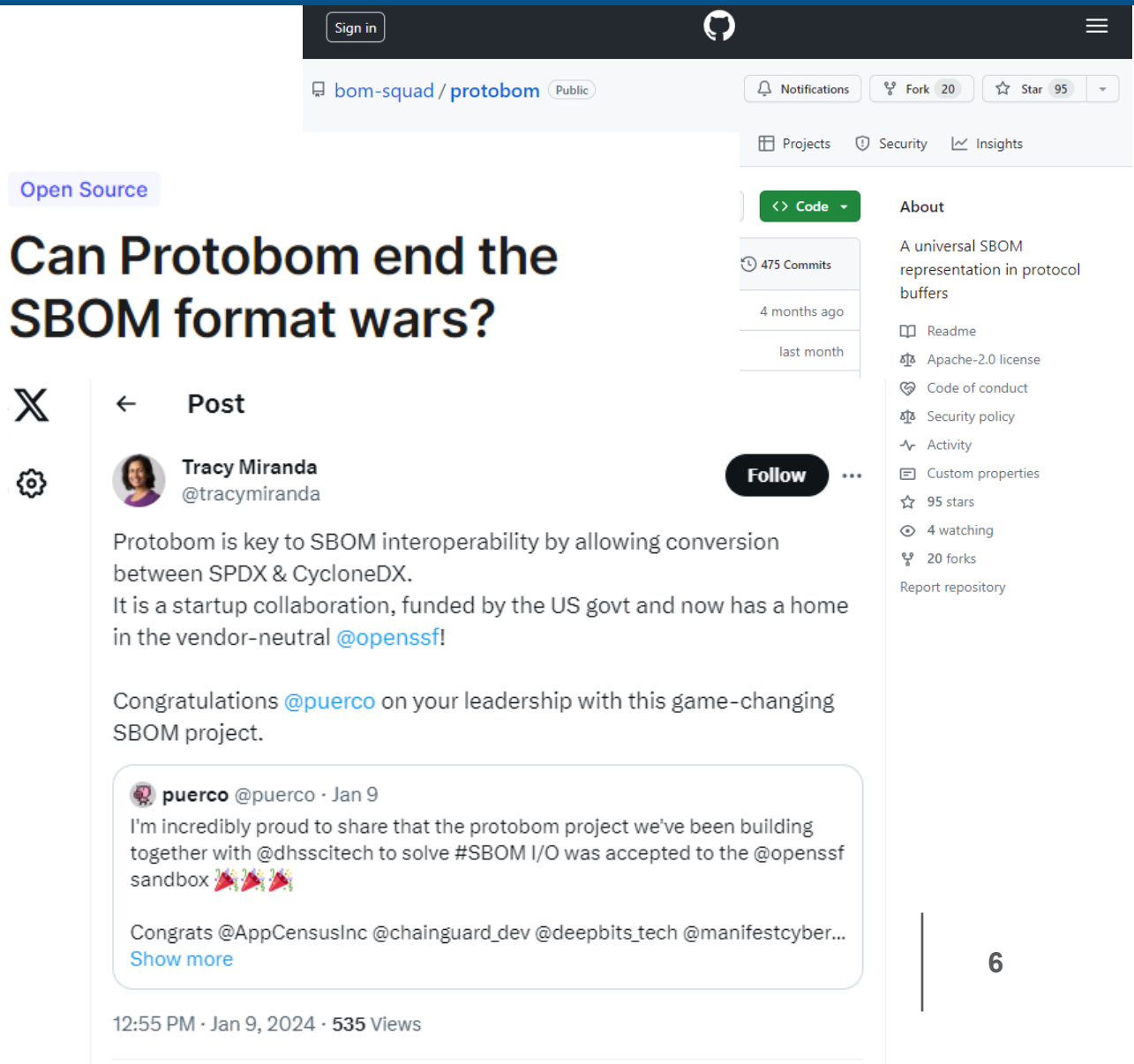
- Manifest
- TestifySec

- AppCensus
- Manifest
- Scribe
- TestifySec

Science & Technology

DHS Expectations; Fulfilled! ☺

- ✓ The open-source codebase developed in Phase 1 will be contributed to an entity who can support community development … globally!
  - ✓ https://github.com/ossf/tac/blob/main/process/project-lifecycle-documents/protobom_sandbox_stage.md
- ✓ Funded companies REQUIRED to incorporate the open-source libraries into their commercial products
- ✓ Phase 2 anticipated very soon!



Privacy Preserving Digital Credential Wallets & Verifiers
Open Global Solicitation in 2023

1 – Digital Wallet
SHALL incorporate one or more OSL(s)

2 – Mobile Verifier
SHALL incorporate one or more OSL(s)

Open-Source Libraries (OSLs)

- OSL (A) – Cryptographic Tools SDK
- OSL (B) – Sealed Storage SDK
- OSL (C) – Metadata Management SDK
- OSL (D) – Confidentiality and Integrity Protected Computing SDK

PRIVACY PRESERVING DIGITAL CREDENTIAL WALLETS & VERIFIERS

Privacy Office

U.S. Customs and Border Protection

U.S. Citizenship and Immigration Services

DHS 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

For more information:
www.cisa.gov

Questions?
Email: Katharine.Mann@cisa.dhs.gov

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

CONNECT WITH SVIP

dhs.gov/science-and-technology/svip

DHS-Silicon-Valley@hq.dhs.gov

dhsscitech


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY