Silicon Valley Innovation Program
Software Supply Chain Visibility Tools
Virtual Industry Day

We will begin promptly at
12:30 pm ET / 9:30 am PT

Science &
Technology

Silicon Valley Innovation Program Software Supply Chain Visibility Tools Virtual Industry Day

July 14, 2022

Science & Technology

Agenda

- Welcome and Introductions
- Keynote
- Software Supply Chain Visibility Challenges and Use Cases
- Technical Topic Areas
- Q&A Session
- Silicon Valley Innovation Program: How DHS Works with Startups
- Adjourn

Housekeeping

- Questions
  - 2 Q&A Sessions:
    1) Software Supply Chain Visibility Tools Use Cases & TTAs
    2) Silicon Valley Innovation Program/How to Apply
  - Please submit your questions into Q&A Box. Where applicable, please identify which speaker your question is directed.
- Presentation and recording will be available next week
- Topic Call details: https://go.usa.gov/xJYgF

DHS Mission & Agencies

FEMA

U.S. Citizenship and Immigration Services

U.S. Immigration and Customs Enforcement

Keynote

Martin Stanley

Strategic Technology Branch Chief, CISA

Science & Technology

Software Supply Chain Visibility Challenge and Use Cases

Allan Friedman, Senior Advisor, CISA

Science & Technology

Silver

Bullet for

Omniscient Risk

Management

Silver

Bullet for

Omniscient Risk

Management

The data layer from software transparency will enable a growing set of use cases and intelligence-driven risk management behavior.

A bit of history

- SBOM is not a new concept
  - Chicken-and-egg problem
  - Need for a shared vision
- NTIA process (2018-2021)
  - What
  - Why
  - How
  - Support implementation
- Executive Order 14028

Executive Order 14028 (May 12, 2021) “Improving the Nation’s Cybersecurity”

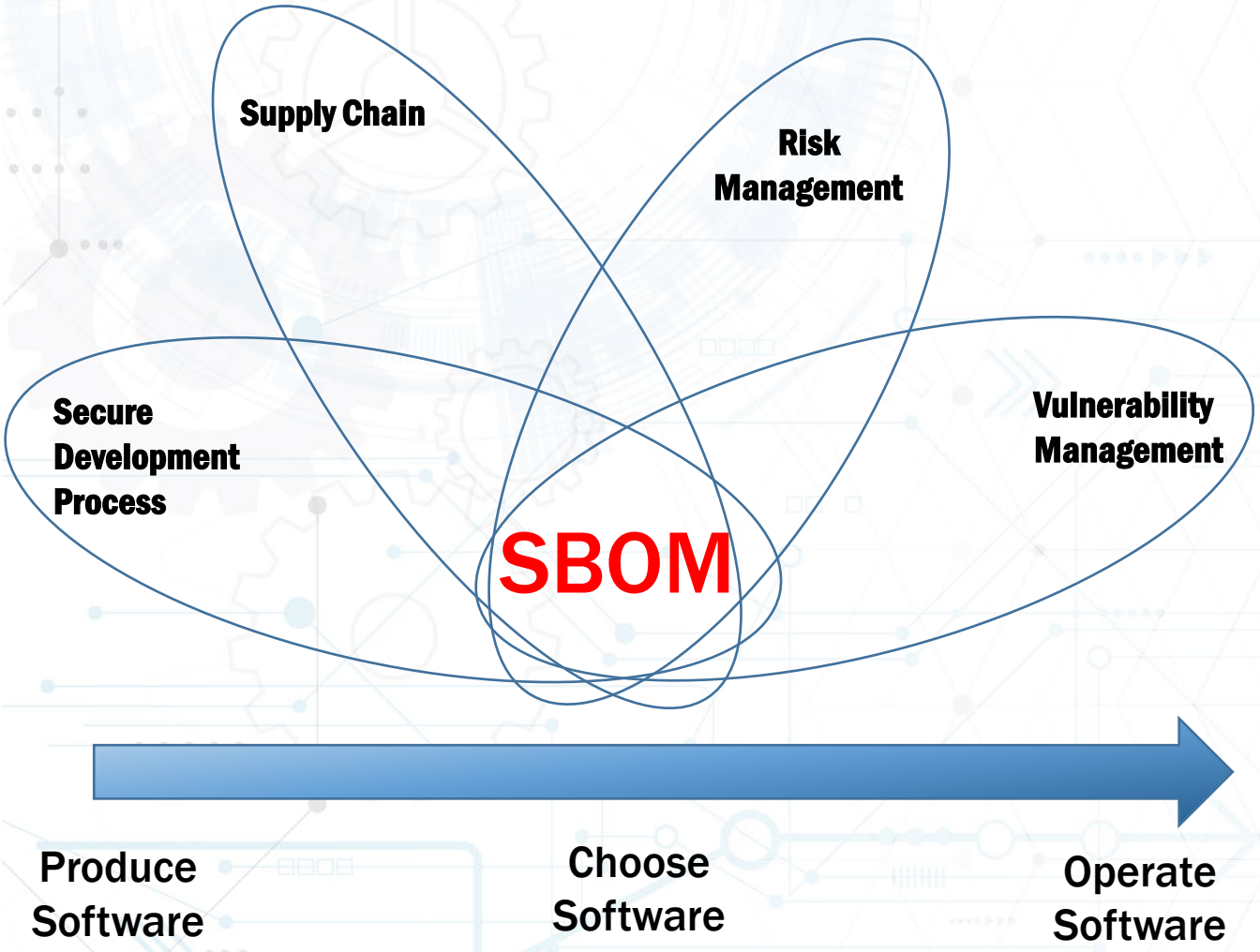
- "The trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is...”
- The EO defines SBOM and identifies the value proposition in 10(j)
- Section 4: Enhancing Software Supply Chain Security.
  - 4(f) – NTIA defines the “**minimum elements**” of SBOM
  - 4(e)(vii) – 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

State of SBOM today

- **SBOM is a more commonly accepted idea across the SW supply chain.**
- **Two widely used data formats and a diverse and growing set of SBOM generation tools.**
- **Proof-of-concept work in a diverse set of industries**
- **Vulnerability Exploitability Exchange (VEX)**

Want to make progress on the scale, operationalization, and seamless integration across the digital ecosystem.

SBOM Roles and Benefits



	Perspective on Software		
Benefit	**Produce**	**Choose**	**Operate**
Cost	Less unplanned, unscheduled work	A more accurate total cost of ownership	More efficient administration
Security Risk	Avoid known vulnerabilities	Easier due diligence	Faster identification and resolution. Know if and where specific software is affected
License Risk	Quantify and manage licenses and associated risk	Easier due diligence	More efficient, accurate response to license claims
Compliance Risk	Easier risk evaluation. Identify compliance requirements earlier in lifecycle	More accurate due diligence, catch issues earlier in lifecycle	Streamlined process
High Assurance (See Appendix II)	Make assertions about artifacts, sources, and processes used.	Making informed, attack-resistant choices about components.	Validate claims under changing and adversarial conditions.

Table 1: Software Bill of Materials - Perspectives and Benefits

https://ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

Motivating Scenarios: Enterprise

Goal: Rapid situational awareness for a new vulnerability

- Integration with asset management
- Mapping known assets to known SBOMs
- Integration with VEX and other attestation data
- Analysis and prioritization of residual risk

Motivating Scenarios: System Administrator

Goal: Understand risk of a new system to the network and organization

- Initial understanding of the dependency graph
- Map SBOM data to datasets of known vulnerabilities or other risks
- Triage risks by prioritization: VEX, active exploitation, etc
- Targeted risk analysis: open source concerns, supply chain concerns, etc
- Integration into broader risk management tools

Motivating Scenarios: Developer

Goal: Easy, hassle-free tools to select & evaluate libraries

- Directly integrates into existing developer tools, complements existing cognitive approaches
- Build out various metrics of code quality and predicted reliability based on SBOM
- Integrated SBOM-driven findings with other data sources
- Collected SBOM data is in turn integrated to the software factory or other build and delivery tool pipelines

Technical Topic Areas

Anil John, Technical Director, SVIP

Science & Technology

Technical Topic Areas

TTA 1 [Required] – Foundational Open-Source Libraries

- Multi-format SBOM Translator
- Software Component Identifier Translator

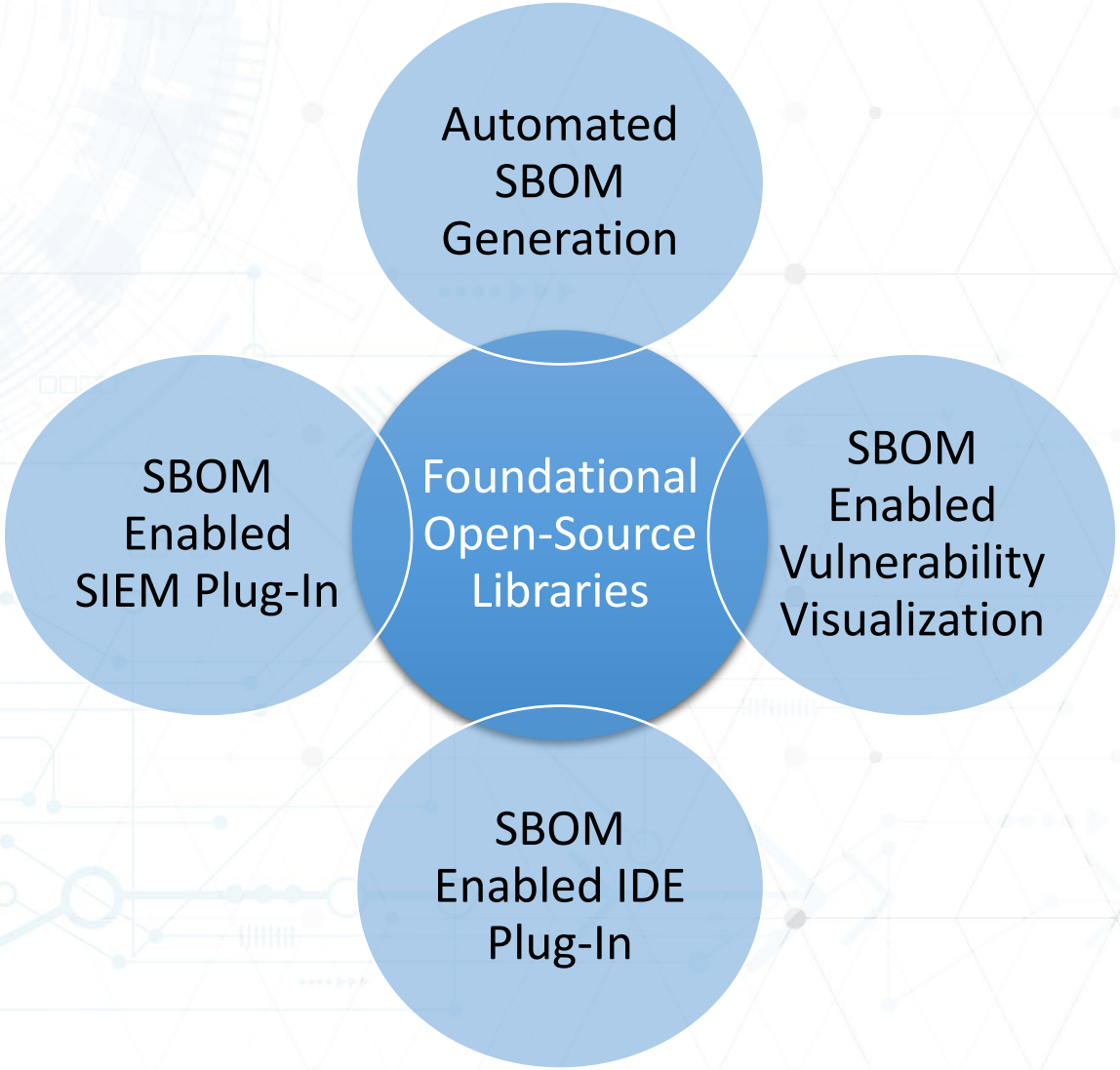
TTA 2 – Automated SBOM Generation

TTA 3 – SBOM Enabled Vulnerability Visualization

TTA 4 – SBOM Enabled IDE Plug-In

TTA 5 – SBOM Enabled SIEM Plug-In

Expectations for TTA Responses



Software Supply Chain Visibility Tools
Q&A Session

Science &
Technology

Silicon Valley Innovation Program

How DHS Works with Startups

Melissa Oh, Managing Director, SVIP
DHS Science & Technology

https://www.dhs.gov/science-and-technology/svip

Science & Technology

Silicon Valley Innovation Program

- Founded in 2015
- Expands DHS's reach to find new technologies that strengthen national security with the goal of reshaping how government, entrepreneurs and industry work together to find cutting-edge solutions

Cultivate
Educate the innovation community on DHS's mission and challenges.

Innovate
Leverage commercial investments & adapt to meet government needs.

- Lowers the barrier to entry for startups globally to work with DHS
- Positioned to address emerging needs rapidly

Benefits

Equity-Free

Network

Mentorship

Market Validation

Amplify Your Reach

Follow-on Funding

By the Numbers

SVIP BY THE NUMBERS

21 TOPICS | **804** APPLICATIONS

137 PHASE 1 PITCHES

65 STARTUPS

32+ M AWARDED FUNDING

163 OTAS

15 COMPLETED/CURRENT PHASE 4 & 5

18 U.S. STATES | **6** INTERNATIONAL

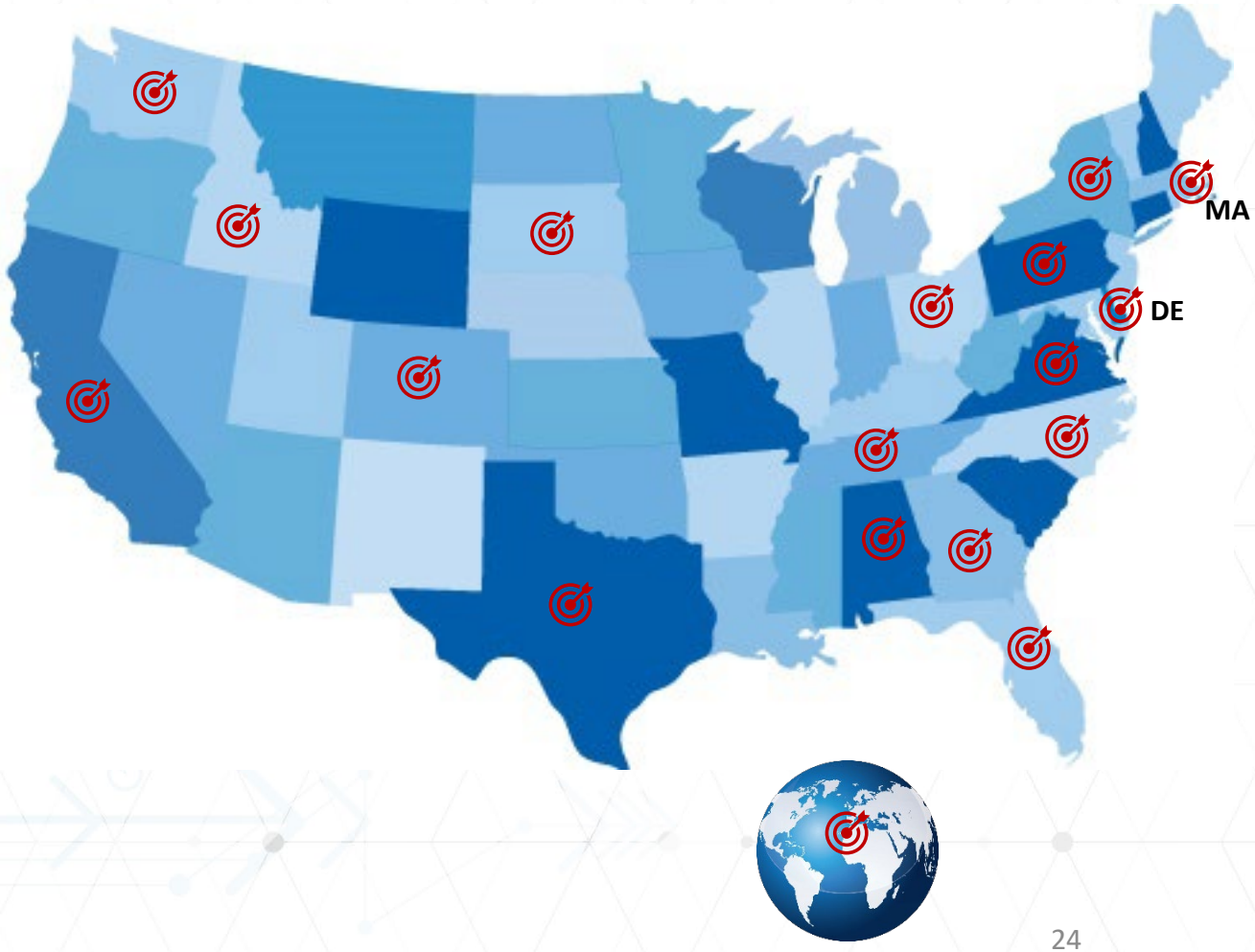
9 FEMALE FOUNDERS

17 MINORITY FOUNDERS

11 TRANSITIONS

53% VENTURE-BACKED

40% POST-SVIP GOVERNMENT CONTRACTS



Past Topics

Internet of Things Security

Big Data

Identity and Anti-Spoofing

Fintech Cybersecurity

Aviation Security

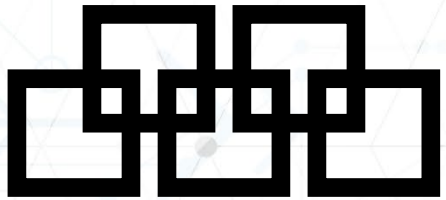
Seamless Travel

Drones/sUAS

K9 Wearables

First Responder Tech

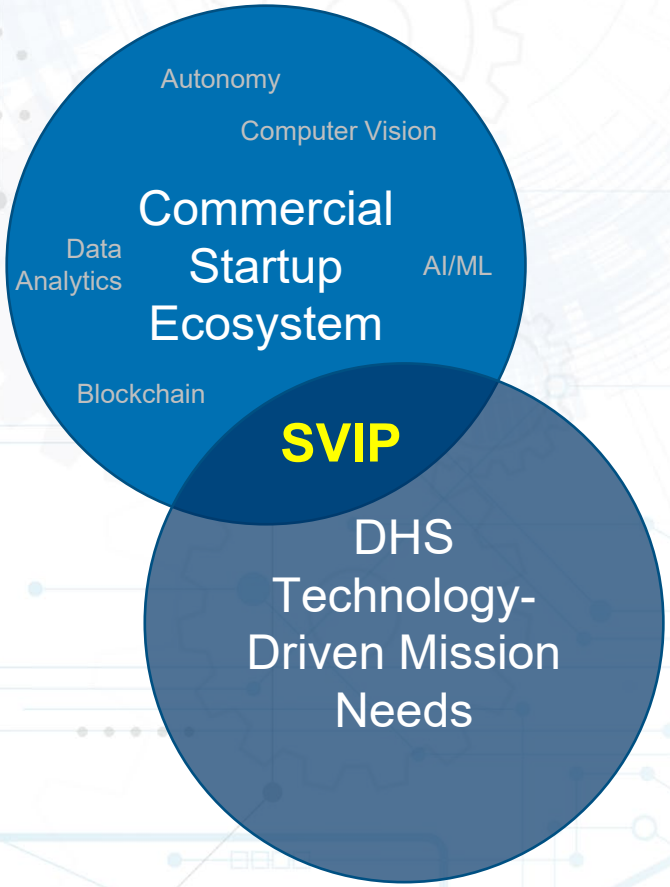
Maritime Security



Blockchain

COVID-19 Response

Eligibility to Participate in SVIP



- Have a Unique Entity ID from SAM.gov. DUNS numbers no longer required as of 4/4/22.
- Have less than 200 employees. This must take into account and include affiliated businesses, such as parent companies and subsidiaries, that are either in or outside of the USA.
- Have not been a party to any U.S. Federal Acquisition Regulation- (FAR) based contracts and/or federally awarded grants totaling more than $1,000,000 in the past 12 months, whether as a prime contractor or subcontractor. This total includes SBIRs.
- Do NOT have any Cost Accounting Standards Contracts with the U.S. federal government

Application Summary

Topic Call

DHS operational agency describes need

Application

Startup submits application laying out how their commercial product can be adapted to meet DHS need

Pitch

Select startups invited to provide 15 minute virtual pitch; Courtesy decision provided within 48 hours

Award

Other Transaction Agreement (OTA) awarded on average within 45 days

Program Summary

Up to $2M over 24 months • 3-4 tranches of non-dilutive funding ($50-500K/3-6 months)

Phase 1
Demo proof of concept

Phase 2
Demo prototype

Phase 3
Functional and Red Team testing

Phase 4
Test in various operational environments

Phase 5
Additional use cases (if requested by DHS)

Demystifying SVIP and Your IP

What DHS Wants	Does NOT Want
• To find innovative companies to help solve challenging homeland security (HS) technological use cases • To lower the barrier of entry for non-traditional companies that may already have viable HS technologies • To match viable HS technologies with a specific DHS or government customer base	• Core Intellectual Property (IP) • All of your proprietary information • To scare off your future investors by tying up your IP • To impede future commercialization of your product(s) or acquisition of your business

IP Rights

- Startup retains ownership of all IP you bring to the project
- Startup gains ownership of all IP created under the OT Agreement
- DHS requires all data to be marked, as is feasible, to ensure appropriate handling

Now What?

Is SVIP for you?

- Am I eligible?
- Do I have a commercial product I'm developing that aligns well with one or more of these use cases?

How do I apply?

- Review the details in the topic call solicitation at: https://go.usa.gov/xJYgF
- Submit your application via the SVIP Portal @ https://svip.dhs.gov/svip/public
  - Deadline: **October 3, 2022** by 12 p.m. Noon PT
  - Do not wait until the last minute to submit. Late submissions and non-compliant applications will not be accepted, no exceptions. Applications are no longer being accepted by email.
- You should hear back within 60 days of the application deadline whether you are invited or not invited to pitch

SVIP Portal

Create an account:

https://svip.dhs.gov/svip/public

Search for Opportunities

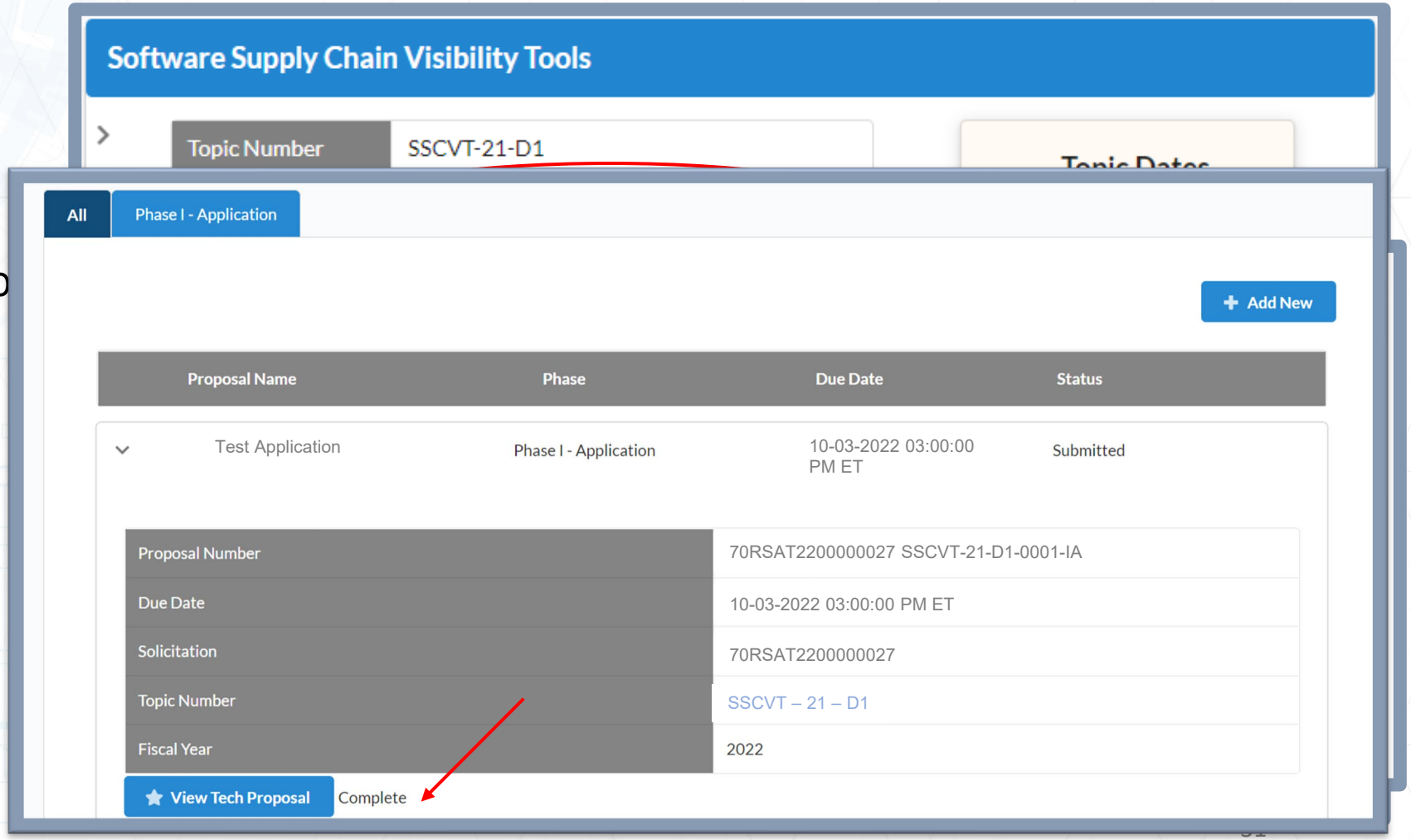
- Software Supply Chain Visibility To
- Click to Apply

Complete Application

- Fill out each tab
- Upload Technical and Cost Volume under Supporting Materials tab

Submit Only 1 Application

- “Complete” once submitted



Milestone vs Deliverable

Milestones

- Notable incremental achievements towards meeting the Phase 1 MVP demo
- Successful milestone completion triggers payment

Deliverables

- The “Deliverables” are the information, items, and materials (data) that are specified in the OT Agreement for delivery to the government
- Startups must NOT deliver to the government any proprietary information, item, or material not specified in the OT Agreement.
- Differentiate between “Deliverable” and “Milestone” when submitting application

Other Things to Know

Exchange & Handling of Sensitive Information

- Limit disclosure of Sensitive Information to the amount necessary to carry out work under this Agreement
- Notices must be prominently placed for all such business sensitive information
- Each party agrees to use reasonable efforts to maintain the security of Sensitive Information
- The obligation to maintain confidentiality expires when the information is no longer deemed by its owner to be Sensitive Information

Acquisition of Your Business or Business Line

- The government needs sixty (60) days notice prior to an acquisition of the entirety of your business or the business line which is responsible for performance of the OT Agreement
- Because there are legal restrictions regarding awarding OTs to nontraditional government contractors, an acquisition of your business by an entity that does not meet that requirement may require terminating the OT
- You must provide information about the specified Deliverables in the OT Agreement and how the government's IP in such Deliverables will be protected
- No specific action is required other than the above

Silicon Valley Innovation Program
Q&A Session

Science & Technology

Thank You for Your Interest!

Can I get a copy of the presentation? Was this event recorded?

- Yes! We will follow-up with an email providing the link of where to access both.

I have more questions. How do I get in touch with the presenters?

- Send us your questions via email to DHS-Silicon-Valley@hq.dhs.gov

My product doesn't meet what you need. How can I find out about other opportunities?

- Check out our other funding opportunities at https://www.dhs.gov/science-and-technology/svip
  - Securing Soft Targets – due Aug 29, 2022 | Flood Data Collection & Analysis – due Sep 2, 2022
- Send us an email at DHS-Silicon-Valley@hq.dhs.gov and ask to be subscribed to our mailing list to hear about other future opportunities
- Check out our sister programs at https://www.dhs.gov/science-and-technology/funding-innovation

CONNECT WITH SVIP

dhs.gov/science-and-technology/svip

DHS-Silicon-Valley@hq.dhs.gov

dhsscitech