Silicon Valley Innovation Program

Privacy Preserving Digital Credential Wallets & Verifiers

Industry Day

We will begin promptly at 11:00 am ET / 10:00 am CT / 8:00 am PT

Science and Technology

Silicon Valley Innovation Program
Privacy Preserving Digital Credential Wallets & Verifiers
Industry Day

18 August 2023

Science and Technology

AGENDA

- Welcome and Introductions
- DHS Challenges and Scenarios Panel Session
- Call Technical Topic Areas
  - Q&A Session
- SVIP: How DHS Works with Startups
  - Q&A Session
- Adjourn

Housekeeping

- Questions
  - 2 Q&A Sessions:
    1. Privacy Preserving Digital Credential Wallets & Verifiers Scenarios & TTAs
    2. Silicon Valley Innovation Program/How to Apply
  - For online, please submit your questions into the Q&A Box. Where applicable, please identify which speaker your question is directed.
- Presentation available now on registration site
- Recording will be available next week on registration site
- Topic Call details: https://bit.ly/SVIP_DigitalWalletsTopic
- WiFi Network: EDPA Guest | Password: guestpassedpa

U.S. Department of Homeland Security Missions & Agencies

1. Counter Terrorism and Prevent Threats
2. Secure and Manage Our Borders
3. Administer the Nation's Immigration System
4. Secure Cyberspace and Critical Infrastructure
5. Build a Resilient Nation and Respond to Incidents
6. Combat Crimes of Exploitation and Protect Victims

U.S. Citizenship and Immigration Services

U.S. Customs and Border Protection

FEMA

CISA
CYBER+INFRASTRUCTURE

Intelligence and Analysis

Management Directorate

Science and Technology

U.S. Immigration and Customs Enforcement

Countering Weapons of Mass Destruction

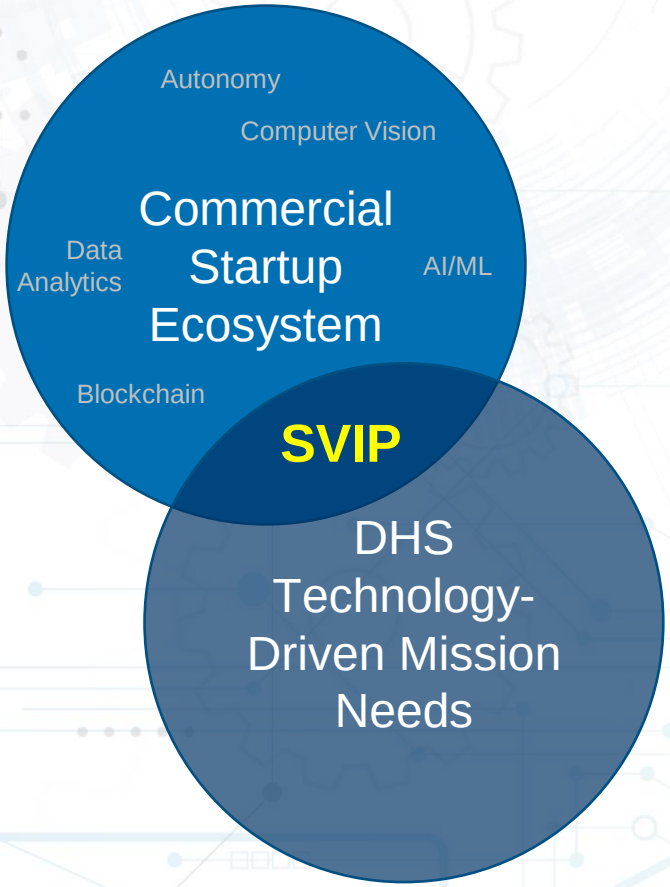
Office of Operations Coordination

Science and Technology

We are the Department's Science Advisor and research and development arm.

Since 2003, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has provided sound, evidence-based scientific and technical perspectives to address a broad spectrum of current and emerging threats.

Silicon Valley Innovation Program



- 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

In 2018, We Released Our Call for "Preventing Forgery & Counterfeiting of Certificates and Licenses"

- DHS Operational Components need to issue, validate and verify entitlements, attestations and certificates
  - Citizenship and Immigration Status
  - Employment Eligibility
  - Essential Work and Task Licenses
  - Organizational Identity & Supply Chain Security
- DHS Operational Components may be both Issuers of Credentials and Validators and Verifiers of Credentials
- **Current issuance processes** are paper based, non-interoperable and susceptible to loss, destruction, forgery, and counterfeiting

PREVENTING FORGERY & COUNTERFEITING OF CERTIFICATES AND LICENSES

- Open Global Solicitation in 2018
- 200+ applications
- **Highly competitive** selection process
- 7 Selected Companies

Now, We are Releasing Our Call for "Privacy Preserving Digital Credential Wallets & Verifiers" to help …

1. Counter Terrorism and Prevent Threats
2. Secure and Manage Our Borders
3. Administer the Nation's Immigration System
4. Secure Cyberspace and Critical Infrastructure
5. Build a Resilient Nation and Respond to Incidents
6. Combat Crimes of Exploitation and Protect Victims

U.S. Customs and Border Protection

U.S. Citizenship and Immigration Services

Privacy Office

Privacy Preserving Digital Credential Wallets & Verifiers

DHS Challenges and Scenarios Panel Session

Science and Technology

Mason Clutter
DHS Chief Privacy Officer

Chris White
Strategic Transformation
Office of Field Operations
U.S. Customs & Border Protection

Jared Goodwin
Chief, Document Management Division
Office of Intake and Document Production
U.S. Citizenship & Immigration Services

Anil John
Moderator
Technical Director, SVIP
DHS Science & Technology

Science and Technology

A Commitment to Privacy, Security, Inclusion and Fair Competition

Encourage and support a plurality of **independent, interoperable, standards-based implementations** to catalyze and operationalize a set of privacy preserving building blocks within the digital credentialing ecosystem

- ✓Support an individual's desire for agency and control in their digital interactions
- ✓Minimize the disclosure of personal data via implementing informed consent management and selective disclosure capabilities
- ✓Eliminate the use of "phone home" architectures, technologies, and implementations
- ✓Ensure that solutions support and enable an ecosystem that is accessible, open, competitive, diverse, and vibrant

Scenario 1: DHS Issuing Credentials to a Digital Wallet

U.S. Citizenship and Immigration Services

- Issue W3C VCDM/DID digital immigration credentials to US Federal, US State, and International Partner Government Digital Wallets that meet DHS requirements

U.S. Customs and Border Protection

- Issue W3C VCDM/DID credentials, for which it is authoritative, into Digital Wallets that meet DHS requirements

Scenario 2: Digital Wallet Holder sharing information with a DHS Verifier

U.S. Customs and Border Protection

- Verify W3C VCDM/DID credentials at web, kiosk, mobile and in-person infrastructure, stored in Digital Wallets that meet DHS requirements, that are needed to enable streamlined cross-border travel

U.S. Citizenship and Immigration Services

- Verify W3C VCDM/DID Credentials at web, kiosk, mobile and in-person infrastructure, stored Digital Wallets that meet DHS requirements, that are required for immigration benefits adjudication

Scenario 3: Digital Wallet Holder sharing information with a non-DHS Verifier

Non-DHS Verifer

- Verify DHS (CBP and USCIS) issued W3C VCDM/DID credentials and other authoritative documentation, stored in Digital Wallets that meet DHS requirements, at non-Government web, kiosk, mobile and in-person infrastructure

Technical Topic Areas
What is DHS Asking for?

Anil John, Technical Director, SVIP
DHS Science & Technology

Science and Technology

DHS and W3C VCDM & W3C DID Standards

W3C Verifiable Credentials Data Model

https://www.w3.org/TR/vc-data-model/#acknowledgements

"Portions of the work on this specification have been funded by the United States Department of Homeland Security's Science and Technology Directorate under contract HSHQDC-17-C-00019."

W3C Decentralized Identifiers

https://www.w3.org/TR/did-core/#acknowledgements

"Portions of the work on this specification have been funded by the United States Department of Homeland Security's (US DHS) Science and Technology Directorate under contracts HSHQDC-16-R00012-H-SB2016-1-002, and HSHQDC-17-C-00019, as well as the US DHS Silicon Valley Innovation Program under contracts 70RSAT20T00000010, 70RSAT20T00000029, 70RSAT20T00000030, 70RSAT20T00000045, 70RSAT20T00000003, and 70RSAT20T00000033."

A (contractually required) Commitment to Standards and Multi-Vendor/Platform Interoperability

Standards Conformance via Automated Test Suites

DHS/SVIP mandates the demonstration of standards compliance using automated conformance test suites

- Contributed to by DHS/SVIP Performers and many others
- Developed under the purview of the relevant SDO (Not DHS)
- With input sought and accepted from the Global technical community

This is not enough!

Multi-Vendor Interoperability via Plug-Fests

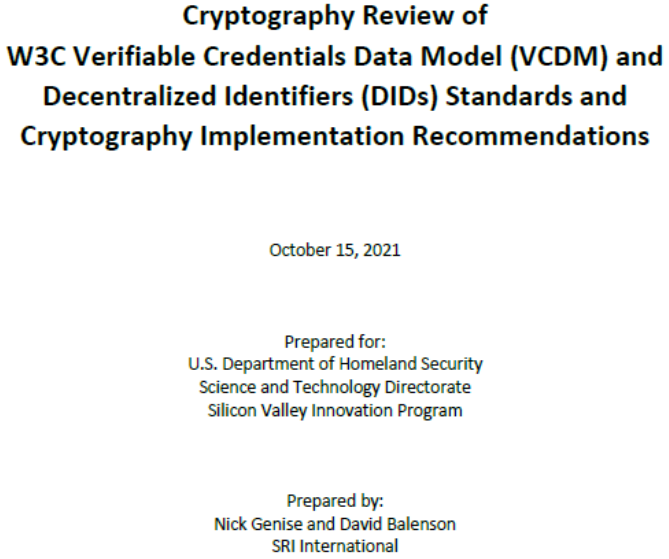
Standards are compromises and as such do not ensure interoperability on their own!

- Standards allow for multiple ways to accomplish the same thing
- Standards allow for multiple ways to represent the same thing

- DHS/SVIP mandates the demonstration of interoperability via a NxN matrix testing of the multiple vendors under contract
- Open to working with non-DHS funded entities in a separate “community plug-fest”

Plug-Fests > to > Scaling Interoperability

- To scale interoperability beyond the just the plug-fest participants, we are documenting the results and lessons from the DHS sponsored multi-platform, multi-vendor Interoperability Plug-fests to develop a **“DHS Implementation Profile of W3C Verifiable Credentials and Decentralized Identifiers”** to ensure the use of Security, Privacy and Interoperability implementation choices that are acceptable to the USG, and can be utilized by anyone
  - *NOTE: A “profile” of a standard remains fully standard compliant but makes explicit choices within the scope of the standard to satisfy specific security, privacy and interoperability criteria. At a minimum, we are using as input:*
    - W3C Verifiable Credentials Data Model
    - W3C Decentralized Identifiers
    - …
- Practical Testing of the USG required cryptography as recommended by an independent cryptography review of W3C VC & DID standards
  - http://www.csl.sri.com/papers/vcdm-did-crypto-recs/
- Demonstrate the Incorporation of Digital Wallet UI Prize Challenge Lessons Learned
  - https://github.com/DHS-SVIP/digital-wallet-ui



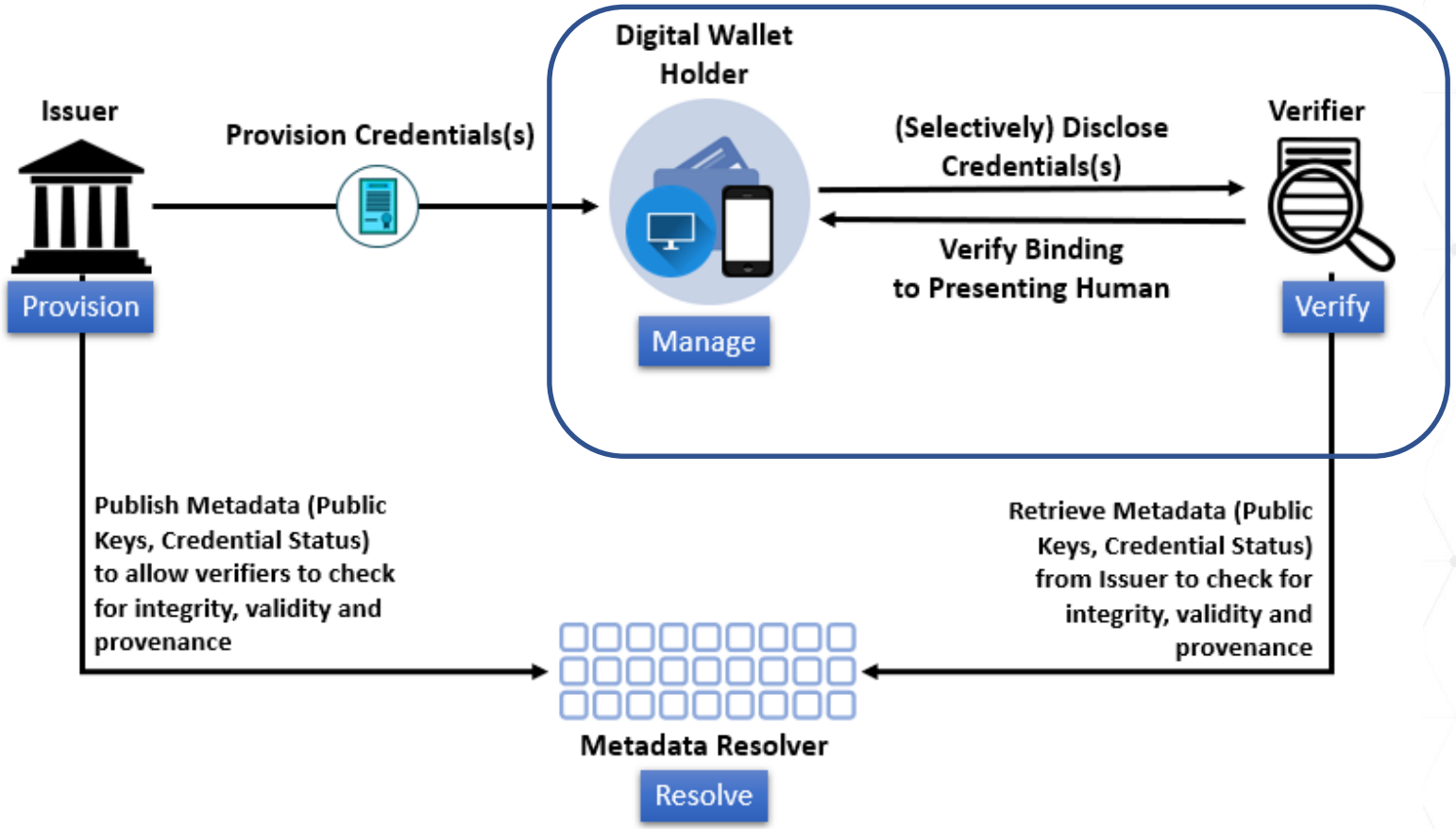
Cryptography Review of
W3C Verifiable Credentials Data Model (VCDM) and Decentralized Identifiers (DIDs) Standards and Cryptography Implementation Recommendations

October 15, 2021

Prepared for:
U.S. Department of Homeland Security
Science and Technology Directorate
Silicon Valley Innovation Program

Prepared by:
Nick Genise and David Balenson
SRI International

Now in 2023, Privacy Preserving Digital Credential Wallets & Verifiers



- The W3C VC Data Model Standard identifies an abstract component called a “Verifiable Data Registry” which in our implementation we refer to as a “Metadata (or Public Key) Resolver”
- We support a Bring-Your-Own-W3C-DID-in-Digital-Wallet for personal credential implementations

Vendors build products …
But ecosystems need building blocks …

… to make hard things easy
… to ensure they are vibrant and interoperable
… to build-in and not bolt-on privacy and security

We seek to enable both products & building blocks!

Privacy Preserving Digital Credential Wallets & Verifiers

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

TTA 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

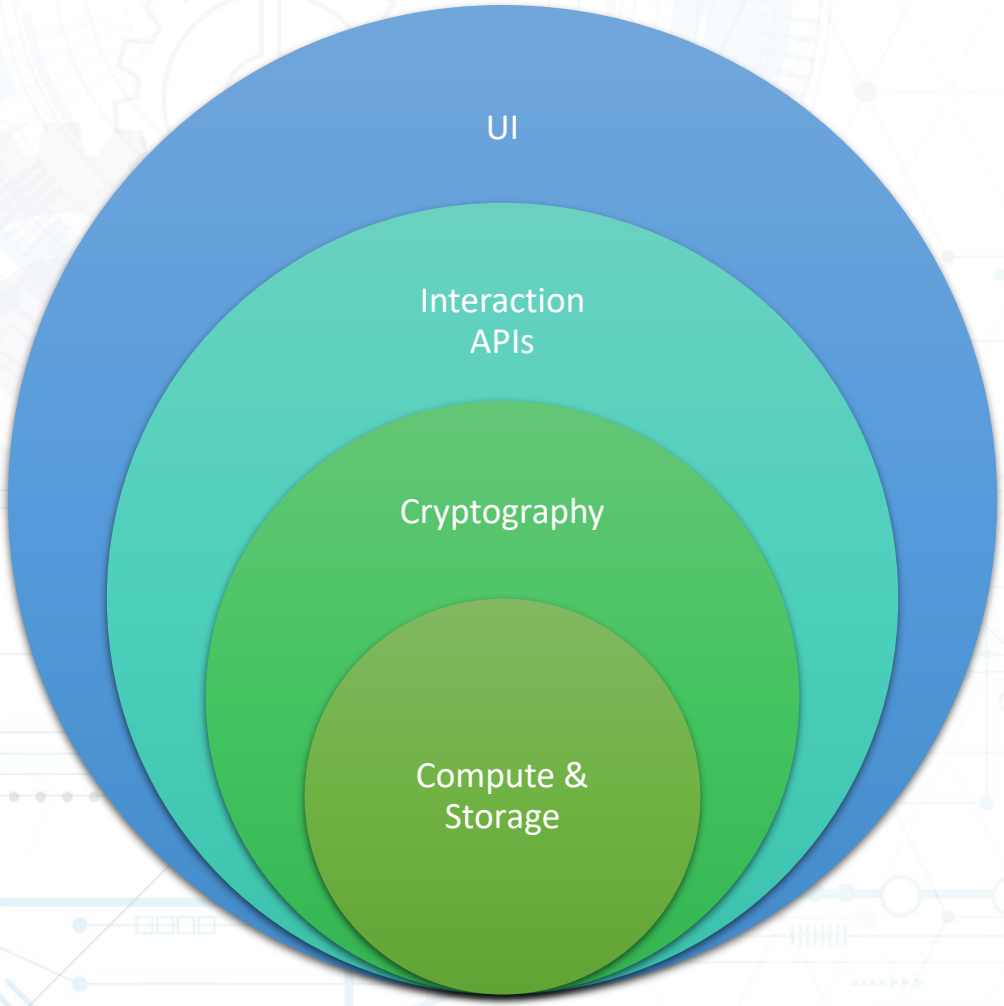
Homeland Security

DHS S&T Silicon Valley Innovation Program (SVIP)

PRIVACY PRESERVING DIGITAL CREDENTIAL WALLETS & VERIFIERS

- Open Global Solicitation
- Application Information @ sam.gov
- Application Deadline is 15 September 2023 12:00 PM PT

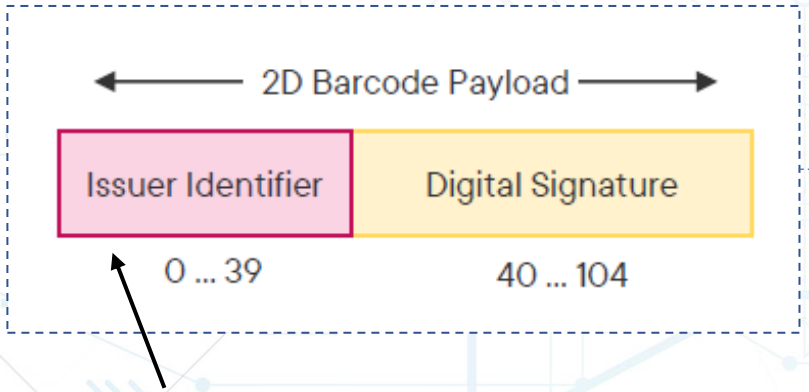
Privacy Preserving Digital Wallet focus on Core Functionality and not Protocols or UI



- UI
  - Branding
  - Consent
  - Aggregation
  - Selective Disclosure
- Interaction APIs
  - Issuer <> Wallet <> Verifier Protocols
  - **Metadata Management SDK**
- Cryptography
  - **Cryptographic Tools SDK**
- Compute and Storage
  - **Sealed Storage SDK**
  - **Confidentiality and Integrity Protected Computing SDK**

Privacy Preserving Mobile Verifier Support for Paper Based Credentials and W3C VCDM/DID Credentials

Digital Signature Payload (Only the data on the card; not the photo)



e.g. did:web:www.uscis.gov

2D Barcode on the physical credential (replaces the fingerprint) contains the issuer identifier and a detached digital signature

- **Issuer Identifier (DID:WEB) is used to resolve to the USICS public key, that can be used to verify the detached digital signature**
- **Detached digital signature contains encoded data attributes present on the physical credential**

- New content integrity and origin authenticity features on the physical PRC.
- USCIS continues to have no awareness of credential usage by a Customer
- No remote calls necessary – USCIS public keys can be downloaded and cached on the verifying device, using the resolver functionality standardized in the W3C Decentralized Identifiers standard, to allow verification to occur without needing to make remote calls to obtain the required public key.

Assumptions and Constraints (See solicitation for complete details …)

Proposed solutions and implementations SHALL be limited to those that support the W3C VCDM Credential Data Model Representation Syntax and W3C VCDM Credential Data Model Proof Formats required by the "*DHS Implementation Profile of W3C VCDM and W3C DID*" utilized by USCIS and CBP

- Support for selective disclosure capabilities to provide the holder of the credential granular control over what information they can share and when;
- Elimination of "phone home" architectures, technologies, and implementations;
- Elimination of "back-channel" interactions between verifiers of the credentials and the issuers which are not visible to the credential holder; and
- Support for open, standards-based digital wallets that do not require a MOU/business relationship with the wallet vendor or require the use of proprietary digital wallet APIs.

Assumptions and Constraints (See solicitation for complete details …)

- All Holder APIs SHALL be publicly documented, patent free, royalty free, non-discriminatory, available to all, and free to implement using widely available and supported programming languages.
- The solution SHALL support Federal Information Processing Standard (FIPS) compliant cryptographic algorithms for hashing, encryption, digital signatures, random number generation and any other relevant cryptographic operations that are performed as part of the solution to ensure its ability to be operationally deployable on a US Government network.
- The Holder SHALL have the ability to choose and utilize (register, select, use) one or more digital wallets that meet openly defined and testable security, privacy and interoperability considerations of Issuers and Verifiers to store and present credentials.

FYI

- DHS/SVIP Red Team testing (in Phase 3) will include an in-depth, **independent code review of the Open-Source SDKs**; DHS will broadly socialize and seek feedback on the results of the code reviews.
- The operational testing and demonstrations (in Phase 4) may include **interoperability testing and plug-fests with International Government Partners** e.g., Government of Canada, the EU/EC and others, who are developing and deploying similar capabilities in order to ensure global interoperability across jurisdictions.

Privacy Preserving Digital Credential Wallets & Verifiers

Q&A

Science and Technology

Silicon Valley Innovation Program
How DHS Works with Startups

Melissa Oh, Managing Director, SVIP
DHS Science & Technology

Science and Technology

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

Benefits

Equity-Free

Network

Mentorship

Market Validation

Amplify Startup Reach

Follow-on Funding

Past Topics

Internet of Things Security

Big Data

Identity and Anti-Spoofing

Fintech Cybersecurity

SW Supply Chain Visibility

Aviation Security

Seamless Travel

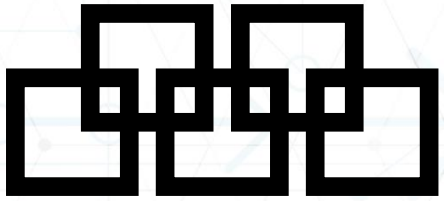
Drones/sUAS

K9 Wearables

Human Performance & Resilience

First Responder Tech

Maritime Security



Blockchain

COVID-19 Response

Flood Analytics

By the Numbers

SVIP BY THE NUMBERS

22 TOPICS | 858 APPLICATIONS

164 PHASE 1 PITCHES

80 STARTUPS

202 OTAS

45+ M AWARDED FUNDING

26 COMPLETED/CURRENT PHASE 4 & 5

20 U.S. STATES | 7 INTERNATIONAL

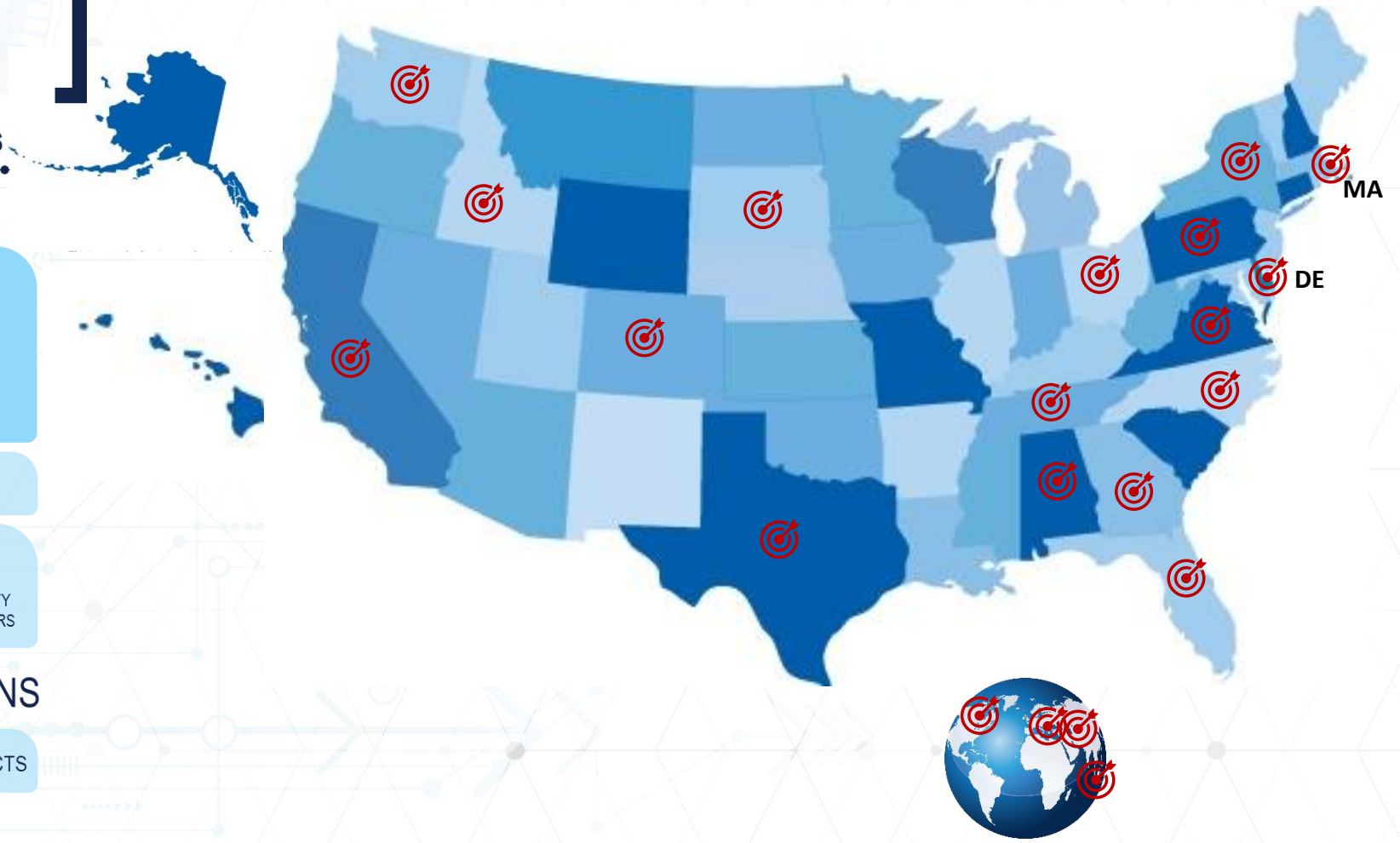
11 FEMALE FOUNDERS

19 MINORITY FOUNDERS

11 TRANSITIONS

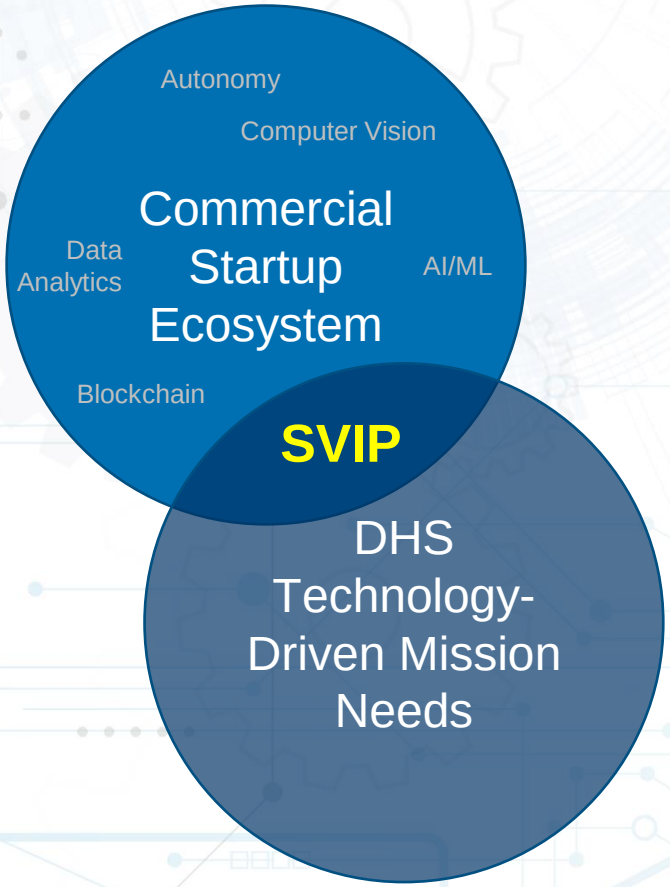
56% VENTURE-BACKED

40% POST-SVIP GOVERNMENT CONTRACTS



Data as of 13 August 2023

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 10 page 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/3-9 months)

Phase 1
Demo proof of concept

Phase 2
Demo prototype

Phase 3
Functional and Red Team testing

Phase 4
Test in representative 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 @ https://bit.ly/SVIP_DigitalWalletsTopic
- Submit your application via the SVIP Portal @ https://svip.dhs.gov/svip/public
  - **Deadline: 15 September 2023 by 12 p.m. 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

- Click "Start Finding Opportunities Now"
- The Privacy Preserving Digital Credential Wallets & Verifiers Solicitation is currently the only open Topic Call and will appear by default
- Click on the blue "Apply" button

Complete Application

- Fill out each tab
- Upload Technical Volume and Cost/Schedule 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

Science and Technology

Thank You for Your Interest!

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

- Yes! Check back on the registration website. Presentation is currently available, recording will be available next week.

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

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

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

- Send us an email at DHS-Silicon-Valley@hq.dhs.gov and ask to be subscribed to our mailing list to hear about future opportunities
- Check out our sister programs at https://www.dhs.gov/science-and-technology/funding-innovation
- Other Funding and Partnership Opportunities at https://www.dhs.gov/science-and-technology/funding-and-partnership-opportunities

CONNECT WITH SVIP

dhs.gov/science-and-technology/svip

DHS-Silicon-Valley@hq.dhs.gov

dhsscitech

Thank You For Attending Industry Day!

Visit the event page to access today's presentation.

Updates, including today's event recording and instructions on how to access FAQs and submission requirements will be posted next week.

Email SVIP at dhs-silicon-valley@hq.dhs.gov

https://bit.ly/SVIP_DigitalWalletsTopic

Silicon Valley Innovation Program

Science and Technology