dhs-silicon-valley@hq.dhs.gov

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

INDUSTRY DAY | Blockchain and DLT Call

WELCOME

23 June, 2020

AGENDA

- Welcome and Introductions
- Silicon Valley Innovation Program Overview
- Preventing Forgery & Counterfeiting of Certificates and Licenses Use Case(s) Panel
- Technical Overview
- Break (10 min)
- Q&A Session – DHS Privacy Office
- Q&A Session – USCIS
- Q&A Session – CBP Office of Trade
- SVIP Application Process & Things You Need to Know
- Q&A Session - SVIP
- Wrap Up/Adjourn

dhs-silicon-valley@hq.dhs.gov

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

MELISSA OH | MANAGING DIRECTOR

SVIP Program Overview

What SVIP Does

We help develop and deliver technology that DHS needs
while promoting economic development through startup/small-business growth

We enable the global innovation community
to tackle the hardest problems faced by DHS's operational missions

CULTIVATE

Educate the innovation community on DHS's mission and challenges

INNOVATE

Leverage commercial investments & adapt to meet government needs

SVIP Application Process

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

How SVIP Funds

Up to $800K over 24 months

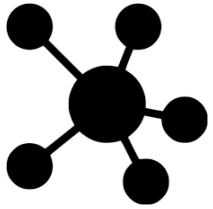
3-4 tranches of non-dilutive funding ❖ Multi-tracking

Performance-based funding steps			
Phase 1	$50-200K	3-6 months	Technology adaptation to address DHS challenge
Phase 2	$50-200K	3-9 months	Full capability build out to demonstrate viability
Phase 3	$50-200K	3-9 months	Capability demonstrations & functional and red team testing
Phase 4	$50-200K	3-9 months	Operational test and evaluation in multiple user scenarios

Benefits to Our Portfolio Companies

Equity-Free

This is a performance-based award. Up to $800K available for every company.



Network

Instant access to DHS public private partnerships and the greater homeland security enterprise, a $544B marketplace.

Mentorship

Learn from the best. We have a deep bench of government and private sector partners who can offer guidance and introductions.

Market Validation

Find market fit through prototype testing and pilot opportunities.

Amplify Your Reach

Demo your product to government, industry and investors from across the world.

Follow-On Funding

Our alumni have received follow-on funding by venture capital investors.

SVIP Portfolio

Internet of Things Security

Big Data

Identity and Anti-Spoofing

Fintech Cybersecurity

Aviation Security

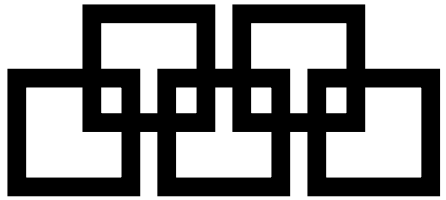
Seamless Travel

Drones/sUAS

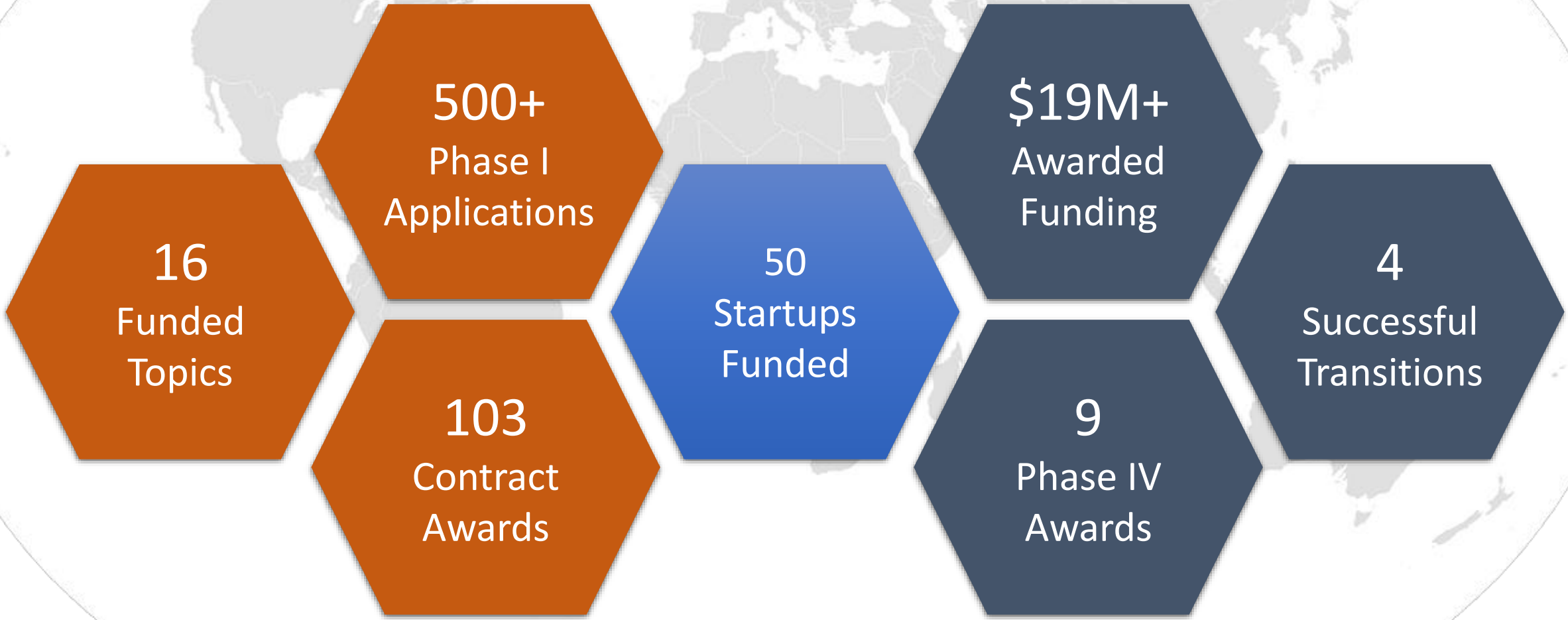
K9 Wearables

First Responder Tech

Maritime Security



Blockchain


16
Funded
Topics
500+
Phase I
Applications
103
Contract
Awards
50
Startups
Funded
$19M+
Awarded
Funding
9
Phase IV
Awards
4
Successful
Transitions

Future SVIP Funding Opportunities?

Learn About Future SVIP Calls (Funding Opportunities)

Request to be Added to our low-volume Notification List by emailing DHS-Silicon-Valley@hq.dhs.gov

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

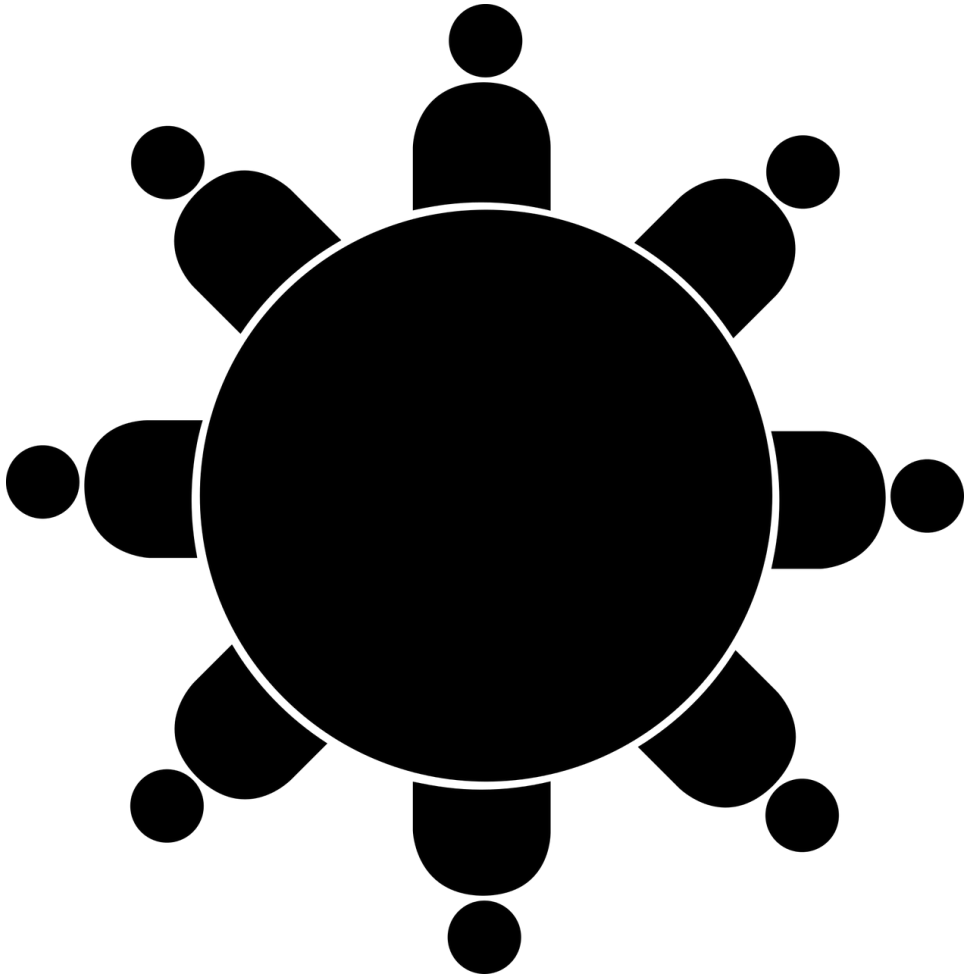
Use Case Panel

Setting the stage

- DHS Operational Components and Programs have different missions; As such their Use Cases and Needs are different
  - DHS Privacy Office (PRIV)
    - Responsible for preserving and enhancing privacy protections and promoting transparency in Department operations
  - U.S. Citizenship and Immigration Services (USCIS)
    - Administers the nation's lawful immigration system and is responsible for the issuance of documentary evidence of citizenship, immigration, and employment authorization.
  - U.S. Customs and Border Protection (CBP)
    - CBP Office of Trade facilitates legitimate trade, enforces law, and protects the American economy to ensure consumer safety and to create a level playing field for American businesses.
- SVIP partners with innovation communities globally to adapt, develop and harness cutting-edge technologies to help solve the problems of DHS Operational Components and Programs

Operational Component & Program Panel

- DHS Privacy Office
  - **David Lindner**
  - **Steve Richards**
- U.S. Citizenship and Immigration Services
  - **Jared Goodwin**
  - **Won Choe**
- U.S. Customs and Border Protection
  - **Vincent Annunziato**



Moderator

Anil John, Technical Director, SVIP

Alternative Identifier to the Social Security number

Privacy Office

Privacy Office has initiated a Social Security Number (SSN) reduction initiative that requires the use of a unique alternative identifier to the SSN. Seeking technologies via this Call that ensure:

- The alternative identifier is meaningless by itself, but globally unique;
- The alternative identifier does not leak personally identifiable information (PII) or information considered sensitive by a person or DHS;
- Public exposure of the alternative identifier does not allow for it to be used as an authenticator or shared secret;
- When needed and allowed by policy, the alternative identifier can be shared and resolved across systems, agencies and organizations without compromising its security and privacy properties; and,
- The alternative identifier is based on global standards to ensure interoperability across and availability within diverse future COTS products.

Privacy Respecting Essential Work and/or Task License

U.S. Citizenship and Immigration Services

USCIS administers the nation's lawful immigration system. There continues to exist the need for individuals to interact in-person with DHS to conduct official tasks, duties and appointments while ensuring public health and safety. The application of technologies sought in the topic call could potentially enhance DHS capabilities to:

- Assert and validate the eligibility of individuals conducting official tasks such as applicants for citizenship, asylum, and other immigration benefits who need entry to DHS offices for the purpose of conducting these official tasks.
- Enable digital representations of currently paper based documentation such as vaccination records or medical releases in a manner that preserves security and ensures the privacy of the individual.
- Assert and validate the eligibility of persons conducting travel designated as essential
- Assert and validate the eligibility of persons conducting business designated as essential

Food Supply Chain Safety and Visibility

U.S. Customs and Border Protection

CBP along with Partner Government Agencies (PGA) are in charge of protecting U.S. consumers from entering illegal and harmful food products. Validating the point of origin for food products by CBP and Partner Government Agencies requires costly inspection and cannot be implemented at scale. The application of technologies sought in the topic call could potentially enhance the CBP capabilities to:

- Enhance the visibility of food supply chains (from farm to point of purchase)
- Enable the application of appropriate duties.
- Reduce spoilage and waste.
- Reduce paper documents.
- Expedite inspection times.
- Enhance targeting.

Supply Chain Traceability of Natural Gas Imports

Validating point of origin and supply chain traceability is complex within continuous flow imports such as natural gas. Natural gas purchases are displacement based, and fluctuations in demand lead to additional complexity import/export declarations. The application of technologies sought in the topic call could potentially enhance CBP capabilities to:

- Allow paperless identification of private sector and government actors related to natural gas exchange
- Facilitate communication between national, state/provincial governments, and private sector entities
- Increase transparency in natural gas exchange between Canada and the US
- Connect supply chain documentation (ex. purchase orders, bills of lading) to related import/export declaration
- Accounting for en route storage and resale
- Simplified in-bond processing
- Avoiding OFAC violations
- Standardized / streamlined reporting in all CBP ports of entry
- Simplified USMCA Claims and Verifications
- Reduced exposure to customs errors caused by third parties

Supply Chain Traceability of Direct-to-Consumer E-Commerce Shipments

U.S. Customs and Border Protection

CBP must adapt to the changing ways business is conducted due to the increasing volume of low-value packages, driven by direct-to-consumer e-commerce. The unprecedented growth in volume of these low-value shipments requires creative solutions to interdict illicit and dangerous products to enter the United States, including illicit narcotics, unregulated prescription drugs, brand counterfeits, and unsafe food and beauty products. The application of technologies sought in the topic call could potentially enhance the CBP capabilities to:

- Enable Importers/websites/sellers to classify merchandise
- Build in automated Duty payments
- Connect all parties involved in the transaction to build a transparent supply chain
- Traceability of packages from internet purchase to consumer
- This includes shipping for all modes of transportation and postal
- Improve targeting on illicit goods and identify emerging risks
- Ease the burden caused by the increased in quantity of package
- Ensure importers to comply with Customs and other Partner Government regulations, particularly small item sellers that may be unintended importers
- Create a better and more simplified way of entering goods into the US
- De minimus

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

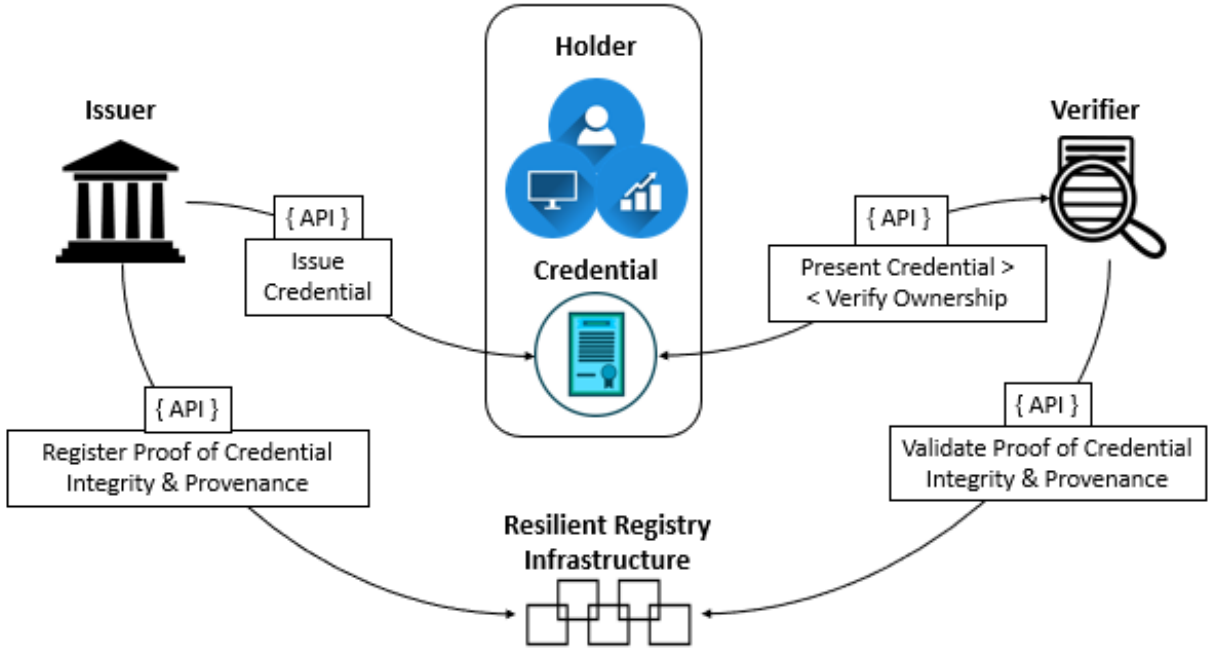
ANIL JOHN | TECHNICAL DIRECTOR

Technical Overview

Scope of Work and Technical Topic Areas

DHS is seeking technologies and solutions that address this need via one or more of the following Technical Topic Areas:

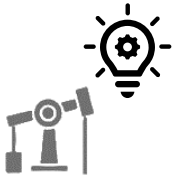
1. Issuance and Verification of Certificates, Licenses and Attestations
2. Storage and Management of Certificates, Licenses and Attestations
3. Decentralized and Derived PIV Credentials



Cross-Border Supply Chain Asset Tracking

Technology Platform X

Oil



Oil Co
extracts crude oil and generates a Verifiable Credential (VC) for it with Platform X's implementation and sends it to the Custom's Broker

1

Customs Broker Co
uses Platform X's HTTP Verifier API to ensure that the **oil** VC signatures are acceptable

2

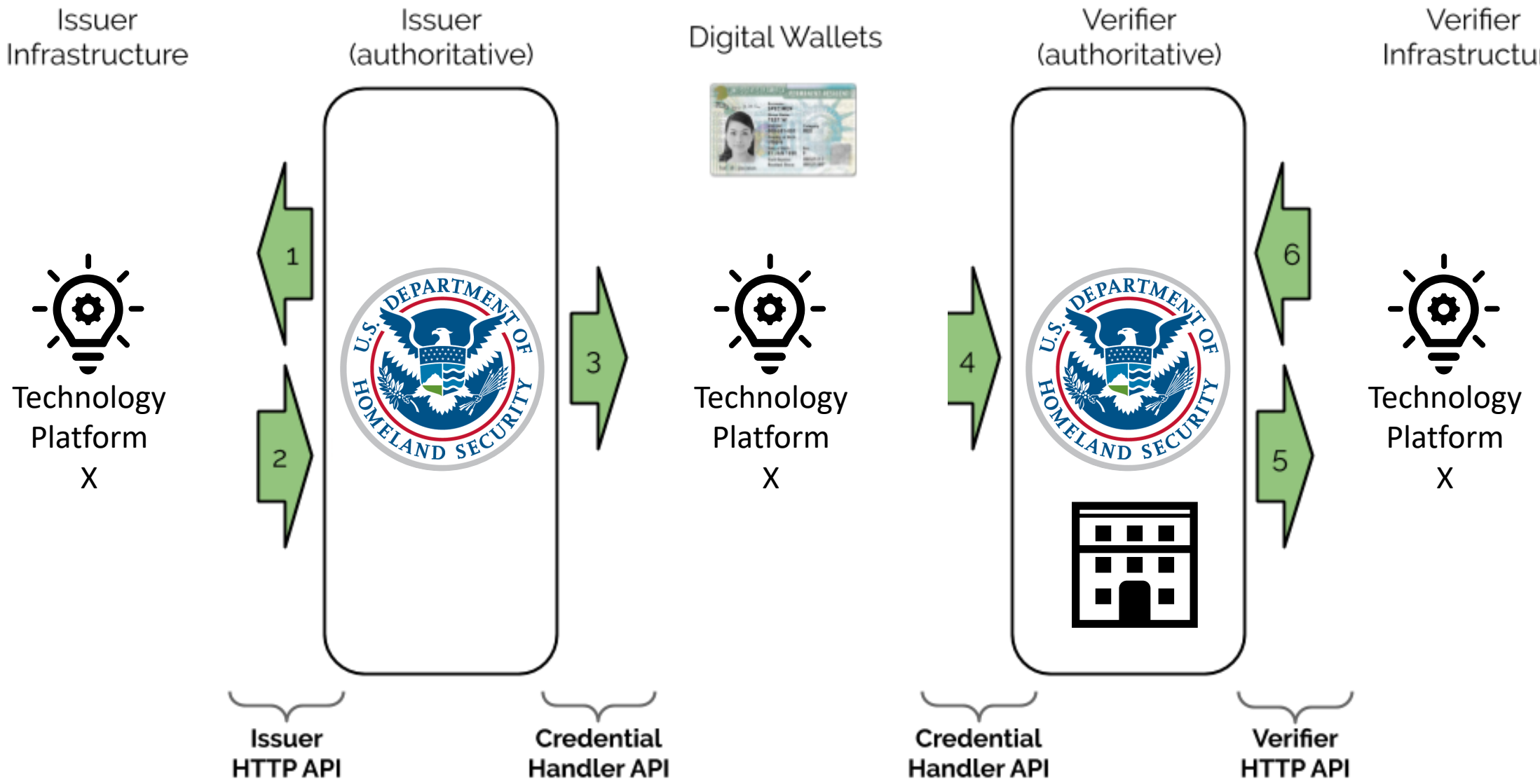
Customs Broker Co
presents the verified products with the VCs to the CBP

3

CBP
uses Platform X's verifier to verify oil

4

Attestation/Credential/Identifier Issuance & Verification



Phase 1 Multi-Vendor Interoperability Plug Fest

6 -7 May, 2020

DANUBE TECH GMBH

Digital Bazaar

SICPA

Mavennet

factom

SECURE KEY

Registry Infrastructure Under Test

- Factom
- Hyperledger Fabric
- Hyperledger Indy
- Mavennet Neoflow
- Transmute for Trade
- Universal Issuer/Verifier
- Veres One

https://lists.w3.org/Archives/Public/public-credentials/2020Jun/0100.html

Interoperable Asset Tracking

Raw material producers (oil, steel and timber) are using different vendors (Mavennet, Transmute, and Factom) to generate VCs specific to the materials they are producing, i.e. Crude Oil Assay, Mill Test Report, Lumber Export Authorization.

Custom Broker uses different vendors to verify VCs presented by each producer

CBP uses yet another vendor to validate the VCs presented by the Customs Broker

Mavennet

Oil

Oil Co
extracts crude oil and generates a Verifiable Credential (VC) for it with Mavennet's implementation and sends it to the Custom's Broker

1a

Customs Broker Co
uses Factom's HTTP Verifier API to ensure that the **oil** VC signatures are acceptable

2a

TRANSMUTE

Steel

Steel Co
manufactures steel and generates a Verifiable Credential (VC) for it with Transmute's implementation and sends it to the Custom's Broker

1b

Customs Broker Co
uses Mavennet's HTTP Verifier API to ensure that the **steel** VC signatures are acceptable

2b

Customs Broker Co
presents the verified products with the VCs to the CBP

3

CBP
uses Mavennet's verifier to verify timber, Factom's to verify steel and Transmute's to verify oil

4

factom

Timber

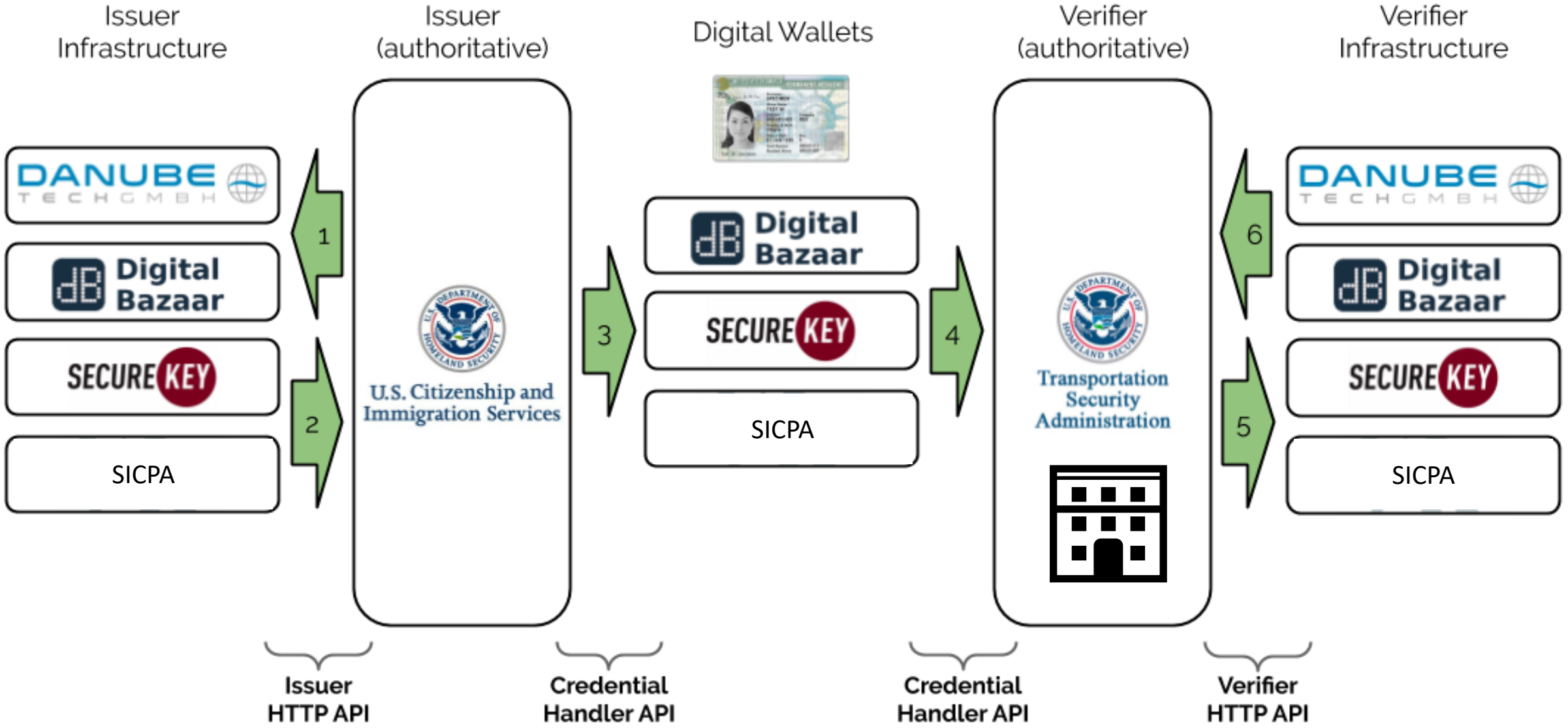
Timber Co
produces timber and and generates a Verifiable Credential (VC) for it with Factom's implementation and sends it to the Custom's Broker

1c

Customs Broker Co
uses Transmute's HTTP Verifier API to ensure that the **timber** VC signatures are acceptable

2c

Interoperable Attestation/Credential/Identifier Issuance & Verification



Homeland Security

DHS S&T Silicon Valley Innovation Program (SVIP)

Phase 1 Multi-Vendor Interoperability Plug Fest

6 -7 May, 2020

DANUBE TECH GMBH

Digital Bazaar

SICPA

Mavennet

factom

SECURE KEY

Registry Infrastructure Under Test

- Factom
- Hyperledger Fabric
- Hyperledger Indy
- Mavennet Neoflow
- Transmute for Trade
- Universal Issuer/Verifier
- Veres One

https://lists.w3.org/Archives/Public/public-credentials/2020Jun/0100.html

Interoperability Guidance to Applicants

… **this call will require any proposed solution to incorporate** the lessons learned from DHS investments in R&D, specifications/standards, and proof-of-concepts that has resulted in **our support for existing and emerging standards-based protocols, data exchange formats and security policy frameworks to ensure interoperable integration with enterprise systems.**

The International Organization for Standardization (ISO) uses specific verbal forms to convey clarity on what is a requirement and what is a recommendation or other type of statement.

We are adopting and using the following ISO document conventions:

- Requirements - SHALL, SHALL NOT
- Recommendations - SHOULD, SHOULD NOT
- Permission - MAY, MAY NOT
- Possibility and Capability - CAN, CANNOT

The SHALLs Applicable to ALL the TTAs …

- All APIs that are presented to the Issuer and the Verifier 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 incorporate, if appropriate to the particular use case, the following emerging and/or mature specifications for interoperability that have been funded, tested and/or championed by DHS:
  - *Decentralized Identifiers (Standards Development Organization - World Wide Web Consortium / W3C)*
  - *Verifiable Credentials (Standards Development Organization - W3C)*
  - *JavaScript Object Notation for Linked Data / JSON-LD (Standards Development Organization - W3C)*

The SHALLs Applicable to ALL the TTAs …

- The Subject SHALL have control over and be accountable for the release of their data (credentials) to the Verifier
- The solution SHALL provide very high resistance to data deletion, modification, masking or tampering e.g. Show equivalency or better between the digital solution and physical security features currently required official licenses and certificates.
- The Identity Verification component i.e. Present Credential / Verify Ownership aspect in the graphic above, SHALL use standardized, strong authentication technologies that is at least Authenticator Assurance Level 2 (AAL2) compliant as documented in *NIST Special Publication 800-63 Revision 3 (or later)*.
- 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.
- The solution SHALL NOT have a dependency on a single Blockchain or DLT implementation.

The SHOULDs Applicable to ALL the TTAs …

- The Subject/Holder SHOULD have the ability to selectively disclose credential information with consent
- The solution SHOULD support online and offline presentation of Credentials to the Verifier
- The solution SHOULD support non-Certificate Revocation List (Non-CRL) based revocation methods (Issuer initiated, Person Initiated, Multi-Sig based and others) that removes Issuer dependencies i.e. “Phone Home Problem”.

Commitment to openness and transparency

"… cohort in concert with the global technical community, has actively worked together in a public and transparent manner to incubate and move into formal W3C standardization pathways via the W3C Credential Community Group (W3C CCG), a set of emerging specifications that ensure global, multi-vendor interoperability for this technology that is a critical requirement of meeting the needs of DHS.

Those standards and emerging include […]

It is expected that any company awarded under this call will actively participate in and support as relevant to their implementation, these emerging specifications as they mature to become global W3C standards"

Objectives for SVIP Phase I

Minimum Viable Product that demonstrates proof-of-concept and supporting documentation inclusive of verifiable test evidence, technical drawings, software or other proof that the technical approach is sound.

Objectives of this phase are to:

- Demonstrate the adaptation of existing technologies to address DHS problem set
- Validate the proposed architecture and design to incorporate interoperability specifications
- Validate digital security criteria equivalency to existing paper based security features.
- Evaluate the design of the APIs
- Evaluate support for Federal Information Processing Standard (FIPS) compliant cryptographic algorithms
- Articulate a go-to-market commercialization strategy

Objectives for SVIP Phase II - IV

Phase II	Phase III	Phase IV
• A working prototype with clearly documented APIs, integrated with a multi-factor authentication mechanism. • End to end application ready for review and evaluation.	• Production ready prototype able to demonstrate all features and functions of the technology. • Ready for red team testing in a realistic deployment environment with an existing issuer and validator infrastructure.	• Red team feedback incorporated into the technology solution and all development is complete. • Ready for operational deployment.

We need your help to solve the business problem!

"The following illustrative scenarios / use cases are intended to describe where the technologies being sought by DHS in this topic call could potentially be applied. DHS is not necessarily seeking the technologies for these specific use cases but instead are providing them to give some context for interested parties.

At the same time, given that responses to this OTS Call may be relevant to these and other use cases, it is expected that an applicant will use one or more of these DHS specific scenarios to frame their application."

This is NOT a R&D funding opportunity.

This is a call for solutions to the business problems we have articulated using the identified technologies, specifications & standards.

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

Break (10 Minutes)
Return @ 1:40 PM ET / 10:40 AM PT

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

Q&A Session – DHS Privacy Office

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

Q&A Session – USCIS

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

Q&A Session – CBP Office of Trade

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

MELISSA OH | MANAGING DIRECTOR

SVIP Application Process

Am I Eligible to Apply?

- Phase 1 applicants must have fewer than 200 employees or full-time equivalents (FTEs)
  - Calculations for FTEs must take into account and include affiliated businesses, such as parent companies and subsidiaries, that are either in or outside of the USA.
- Phase 1 applicants must not been a party to any Federal Acquisition Regulation based contracts and/or federally awarded grants with a combined total of more than $1,000,000 in the past 12 months, whether as a prime contractor or subcontractor.
  - This is across the US Federal Government (not just DHS) and includes SBIRs
  - Must not have any Cost Accounting Standards Contracts with the US Federal government
- All applicants must have a Dun & Bradstreet (DUNS) number
  - You can register for it at www.DNB.com

How Startups Apply to our Program

1. Review the topic call and decide whether your solution applies
2. Submit application via email using provided application form (available with each call) to DHS-Silicon-Valley@hq.dhs.gov
3. If application is selected, (1) Prepare for a 15 minute virtual pitch
   (2) Register in sam.gov; this is how we can pay you
4. If selected for funding, courtesy notification within 48 hours and Awards will contact you
5. Award timeframe estimate is 45 days from date of notification

What DHS wants:

- 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

What DHS does NOT want:

- Your 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

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

Protecting Your Intellectual Property

- We want to protect your core IP
- We don’t want to infringe third party IP rights
- In the process of working with DHS, you may share/create several different types of protectable IP, such as:
  - Trade Secret Information/Data
  - Copyrighted material
  - Inventions and/or patented technology
  - Other types of technical data

IP Architecture

- We want to know what you're bringing to the table
- DHS understands that applications often involve systems, projects, and software previously developed by applicants, whether at private expense or funded through other contracts. If it relates to the proposed project, applicants should diagram what they've previously created and what they're proposing to create under this effort

For instance, if an applicant proposes to create a software module prototype specific to DHS' needs, the applicant could show that the base software package was previously developed at private expense.

It may also show that software libraries used in that base software package are subject to open source software licenses, like BSD or GPL. And it may show that the DHS-specific module/prototype is delivered under this agreement and subject to terms and conditions negotiated in this agreement.

IP Rights

- You retain Ownership of all IP you bring to the project
- You gain Ownership of all IP created under the OT Agreement

DHS requires all Data to be marked, as is feasible, to ensure appropriate handling

IP License

- By submitting the project deliverables, OT Recipient grants to DHS the following:
  1. A paid-up, non-exclusive, irrevocable, royalty-free, worldwide license to use, reproduce, distribute, sublicense, and create derivative works of any reports provided to DHS, its partners, and those working on its behalf.
  2. Reasonable assistance and additional information concerning Work Product/Milestones/Deliverables during the period of performance and up to 3 years after the end of the period of performance.
- In the case where the OT Recipient is demonstrating or otherwise sharing work product, related materials, and know how in connection with the Agreement (including for testing by DHS as may be described in the Statement of Work), OT Recipient grants to DHS the following during the period of performance or as otherwise stated in the Agreement:
  - A nonexclusive, nontransferable, irrevocable, paid-up license to use or practice all work product and related materials by or on behalf of the Government as described in the Statement of Work or as otherwise agreed to in the Agreement

Deliverables

- The “Deliverables” are the information, items, and materials (Data) that are specified in the OT Agreement **for delivery to the Government**
- **Please DO NOT** deliver to the Government any proprietary information, item, or material not specified in the OT Agreement.

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

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

Q&A Session – SVIP

Homeland Security

Science and Technology

Thank You

Silicon Valley Innovation Program

DHS-Silicon-Valley@hq.dhs.gov
https://www.dhs.gov/science-and-technology/svip