Homeland Security

DHS S&T Silicon Valley Innovation Program (SVIP)

PREVENTING FORGERY & COUNTERFEITING OF CERTIFICATES AND LICENSES

Other Transaction Solicitation Call
70RSAT19R00000002

Application Form @ https://go.usa.gov/xPGsr

Register & Attend the Industry Day
11 Dec, 2018 in Menlo Park, CA, USA
(See Section 5.1 for Registration Details)

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

1. Introduction

This Other Transaction Solicitation (OTS) Call 70RSAT19R00000002 is being issued against the Department of Homeland Security (DHS), Science & Technology (S&T), Silicon Valley Innovation Program (SVIP), 5-Year Innovation OTS (HSHQDC-16-R-B0005). All terms and conditions of the DHS S&T SVIP 5-Year Innovation OTS (HSHQDC-16-R-B0005) are incorporated into this Call unless otherwise noted herein.

The U.S. Department of Homeland Security (DHS) is committed to using cutting-edge technologies and scientific talent in its quest to make America safer. The DHS Science and Technology Directorate (S&T) Silicon Valley Innovation Program (SVIP), on behalf of DHS Operational Components, invests in startup companies with viable technologies suitable for rapid prototyping projects from across the nation and around the world to adapt, develop and harness cutting-edge capabilities that are commercially sustainable while simultaneously meeting the needs of DHS Operational Components and Programs.

1.1. DHS Operational Need

Blockchain and Distributed Ledger Technology, from a government perspective, holds the potential for enhanced transparency and auditing of public service operations, greater visibility into multi-party business operations, and automation of paper-based processes to improve delivery of services to organizations and citizens.

DHS Operational Components and Programs have common needs across their mission sets for potential use of interoperable implementations of Blockchain and Distributed Ledger Technologies (DLTs) that also support the growth and availability of a competitive marketplace of diverse technology implementations for government and industry to draw upon to deliver cost effective and innovative solutions.

This SVIP Call seeks technical capabilities that could serve the mission needs of one or more DHS Operational Components and Programs including:

- *U.S. Customs and Border Protection (CBP)*
- *U.S. Citizenship and Immigration Services (USCIS)*
- *Transportation Security Administration (TSA)*

1.2. Illustrative Use Cases

There exists across DHS Components and the Homeland Security Enterprise the need to issue entitlements, attestations and certifications for a variety of purposes including travel, training, education, affiliation, organizational identity and delegated authority and more. Current issuance processes are often paper based, non-interoperable and are susceptible to loss, destruction, forgery, and counterfeiting.

The following illustrative 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 to frame their applications**. Responses to this OTS Call may focus on these and/or other potential use cases.

1.2.1. Hypothetical Scenario I: Identity Documents for Travel

TSA has a responsibility to confirm the identity of each passenger at the TSA security checkpoint and ensure that the identity presented on the digital document matches the identity associated on a confirmed travel reservation. Transportation Security Officers (TSO) currently review credentials (e.g., driver's license), assess them for possible fraud or tampering, manually match the biographic information on the credential and the boarding pass, and visually compare the photo on the credential to the face of the traveler. This manual process needs to be performed in seconds to prevent creating a bottleneck in the queue and is highly reliant on the judgment of the TSO. TSA is moving towards electronic authentication capabilities to strengthen this process in support of TSOs. The application of technologies sought in the topic call could potentially enhance the TSA capabilities to:

- Prove the authenticity and provenance of identity documentation at speed
- Ensure that the digital document has counter-fraud protections to
    - Increase the ease of authentication for the TSA
    - Increase capability to identify indicators of tampering or fraud
    - Increase the costs to actors attempting to spoof/fake the credential
    - Limit/decrease the useful lifetime of documents that are counterfeited
- Direct Passengers to certain screening lanes by applicable risk-based screening protocol (e.g., trusted traveler program participant, standard traveler, etc.)

1.2.2. Hypothetical Scenario II: Identity of Organizations and Organizational Delegates

CBP and other DHS Operational Components have various responsibilities regarding supply chain security and intellectual property rights enforcement. These needs require knowing the identity of organizations that are part of a supply chain and understanding who has been delegated to perform a particular function on behalf of an organization. The application of technologies sought in the topic call could potentially enhance the capabilities available to DHS to ensure the ability to:

- Validate the identity of an Organization
- Validate affiliation of a person to a legitimate Organization
- Ensure that the delegated entity is the actual Person performing the actions on behalf of the Organization

1.2.3. Hypothetical Scenario III: Tribal Identity Documents for Travel

Tribal jurisdictions within the United States have the authority to issue identity documents that TSA may accept for domestic air travel and USCIS may for other uses. The sheer number of federally recognized tribes and types of documents issued presents a challenge to Transportation Security Officers to recognize, validate, and verify tribal documents when encountered at TSA checkpoints. Also, the absence of common issuance and production criteria means the quality of these documents can vary among tribal issuers. While keeping in mind that there are broader legal and policy concerns that need to be addressed for this scenario, TSA and USCIS have an interest in how the technical implementation of a tribal identity document using the technologies sought in this call could meet the following technical criteria:

- The digital document has counter-fraud protections that are equivalent to the security protections required of physical documents.
- The digital document allows the reliant party to distinguish among tribal documents based on pre-determined criteria (e.g., Federal recognition of the tribe, issuance practices, etc.).

- The implementation has the ability to integrate with the current issuance and validation processes

1.2.4. Hypothetical Scenario IV: Citizenship, Immigration and Employment Authorization

USCIS administers the nation's lawful immigration system and is responsible for the issuance of documentary evidence of citizenship, immigration, and employment authorization. The application of technologies sought in this topic call could potentially enhance those capabilities by enabling digital representations of those documents that:

- Provide identity protections that allow for disclosure of information under the control of the owner of the credential
- Provide the ability to remotely mange the lifecycle of the credential (electronic document)
- Integrate with the current secure issuance processes

1.2.5. Hypothetical Scenario V: Cross-Border Oil Import Tracking

Crude oil and oil products crossing the US-Canadian border rely on estimation of pipeline flows for admission and charging of appropriate duties. The same pipeline may be used for different types of oil, with different duties. Additionally, oil imported to Canada may be comingled with Canadian oil for export. The current process for capturing this transaction flow is manual and complex. The application of technologies sought in the topic call could potentially enhance the CBP capabilities to accurate admit oil under USMCA and apply appropriate duties by:

- Accurately tracking the evidence of the flow of oil through pipeline and refinement between the US and Canada
- Attribute oil imports with the accurate composition and country of origin

1.2.6. Hypothetical Scenario VI: Origin of Raw Material Imports

CBP relies on country of origin data from importer documentation. Validating the point of origin for raw materials (ex. timber, diamonds, and precious metals) by CBP requires costly inspection and cannot be implemented at scale. Transit through a nation with a preferential trade agreement could be used to confound the true country of origin, resulting in lost duty revenue and support of illicit activities. The application of technologies sought in the topic call could potentially enhance the CBP capabilities to:

- Track the documentary evidence of the flow of raw materials from the point of extraction
- Enable the application of appropriate duties
- Ensure goods imported to the United States do not come from force labor or fund criminal or terrorist organizations

2. Topic Description

DHS is interested in Blockchain and DLT solutions that address the challenges of interoperable digital entitlement attestations that support individual control and accountability of data release, while incorporating digital counter-fraud technologies and tactics, enterprise lifecycle management, and a high degree of usability across service delivery modalities.

2.1. Interoperability Guidance

Blockchain and Distributed Ledger technologies are still in its infancy, and are currently in a phase

where there is an increasing amount of tension between business/system owners, both in the private sector and public sector, and their technology and solution providers. For example, a technology provider's desire to gain traction for their particular Blockchain implementation may run up against the business/system owner's expectation of having an open architecture environment for their systems, rather than vendor-specific approaches to prevent technology lock-in. Technology providers may recommend a replacement strategy to implement their Blockchain, which runs counter to the business/system owners desire for innovative technology that integrates with their current business processes and technology to preserve and leverage existing investments.

This potential for the development of "walled gardens" or closed technology platforms that do not support common standards for security, privacy, and data exchange would limit the growth and availability of a competitive marketplace of diverse, interoperable solutions for government and industry to draw upon to deliver cost effective and innovative services based on Blockchain and distributed ledger technologies.

Interoperability of technology solutions at global scale typically requires a solution provider to address and make specific choices regarding the protocols, payloads and policies supported by their implementations. While novel and innovative solutions are being sought as part of this topic call, DHS S&T and its mission partners have over the last 3+ years conducted extensive R&D, proof of concepts and community engagement to understand, demonstrate and champion a path that accelerates the development and usage of specifications and standards to foster a baseline of interoperability, security and privacy.

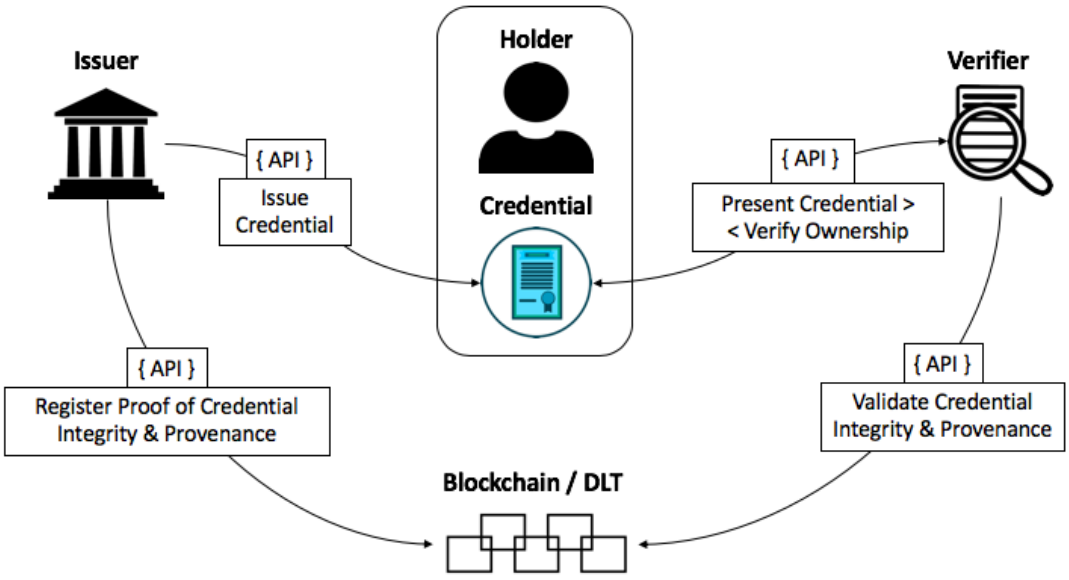
As such, this call will require any proposed solution to incorporate the lessons learned from DHS investments in R&D, specifications/standards, and proof-of-concepts that has resulted in our support for existing and emerging standards-based protocols, data exchange formats and security policy frameworks 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. This Topic Call adopts and uses the following ISO document conventions:

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

2.2. Scope of Work

There are a variety of challenges that must be overcome to provide an equivalent digital capability that supports the multiple entities that are part of any such process while ensuring security, privacy, interoperability and integration with existing back-end processes.



The graphic above provides a high-level and conceptual view of the multiple entities involved in any such process.

Holder	A person, citizen or employee that controls a Digital Wallet or Personal Data Store that stores entitlements, attestations and certifications and key management materials.
Issuer	An authoritative source that is capable of issuing credentials e.g. Government Agency, Employer etc.
Verifier	An entity that validates integrity and provenance of the credentials provided by the Holder and ensures that the credentials asserted belong to and are relevant to that Holder.
Blockchain / Distributed Ledger	The infrastructure that supports the public validation of potentially private data (e.g. credentials) without the need to directly store that data.

There is no expectation that all of the entities in the model above are managed or operated by a single entity but instead represents an ecosystem that enables a pluralism of operators and technologies to ensure interoperability, encourage diversity, and prevent technology lock-in.

Providing Application Programming Interfaces (APIs) that are publicly documented, patent free, royalty free, non-discriminatory and available to all mitigates technology and vendor risk to Issuers and Verifiers while simultaneously providing the technology provider the ability to utilize innovative and possibly proprietary technologies behind the API.

To that end, the following are specific items to be incorporated into each Technical Topic Areas (TTAs) listed below to ensure that solutions are secure, privacy respecting, scalable and interoperable:

- 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 Holder 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 solution SHALL NOT have a dependency on a single Blockchain or DLT implementation.
- The Identity Verification component i.e. Present Credential / Verify Ownership aspect in the graphic above, SHALL use standardized, strong authentication technologies (e.g. FIDO, OIDC etc.) that is at least Authenticator Assurance Level 2 (AAL2) compliant as documented in *NIST Special Publication 800-63 Revision 3* (or later).
- The 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”.
- The solution SHOULD 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.

3. Technical Topic Areas (TTAs)

DHS is seeking technologies and solutions that address this need via one or more of the following TTAs.

While DHS is interested in meeting the goals of all the TTAs, we want to make it clear that is not a requirement and as such you are encouraged to apply even if your prototype project meets only one TTA.

3.1. TTA #1: Issuance and Verification of Certificates, Licenses and Attestations

Issuers are the authoritative sources of any credentials and it is desirable to provide the maximum flexibility in the solutions they can integrate with by ensuring a consistent set of integration points.

The Issuer is expected to integrate with two solution capabilities:

1. Credential Issuance API – Provides a standardized mechanism to issue a Credential to a Holder via a secure process. It is expected that the Credential(s) will be stored and managed in a secure environment that is under the control of the Holder e.g. A hardware wallet, Secure element in a mobile device, etc.
2. Credential Registration API - Provides a standardized mechanism to register the proof of a Credential in a manner that ensures its integrity and validity as of a particular point in time, and its provenance on a Blockchain / DLT that allows for public validation of potentially sensitive Credential data without storing that data directly on a Blockchain / DLT and to validate the source as being the Issuer.

Verifiers are the entities that validate the credentials provided by a Holder and ensure that the Credentials asserted belong to and are relevant to the particular Holder who provides them. As such it is desirable to provide them maximum flexibility in the solutions they can integrate with by ensuring a consistent set of integration points.

The Verifier is expected to integrate with two solution capabilities:

1. Identity Verification (Present Credential / Verify Ownership) API – Demonstrating proof of ownership of a Credential is not a Blockchain specific technology but instead is the application of existing standardized, strong authentication technology. As such it is expected that existing and standardized strong authentication technology SHALL be used (e.g. FIDO, OIDC etc.) that support at least Authenticator Assurance Level 2 (AAL2) compliance as documented in *NIST Special Publication 800-63 Revision 3* (or later).
2. Credential Validation API – Provides a standardized mechanism to validate the integrity of an issued credential as of a particular point in time and to ascertain that a trusted Issuer issued it.

Analysis and recommendations that support and articulate the trade-offs associated with particular implementation choices are an important aspect of the information sought as part of any proposed solution.

3.2. TTA #2: Storage and Management of Certificates, Licenses and Attestations

The Digital Wallet or the Personal Data Store under the control of a Holder can take many forms including hardware tokens, secure elements in mobile devices, secure web application and more.

What has typically been missing from the current implementations has been lifecycle management of such capabilities from an Enterprise perspective combined with the ability to plug in to standardized APIs.

This TTA is directly focused on enabling a set of technologies that deliver the following outcomes:

- Integration with multiple Issuers via standardized APIs
    - Credential Issuance API as noted in TTA #1
    - Proof of Ownership API as noted in TTA #1
- Enterprise managed provisioning, revocation and re-issuance of keys and credentials stored within the Digital Wallet or Personal Data Store
- Support for Enterprise driven key recovery rather than social key recovery mechanisms

Given the criticality of key management to any such Blockchain / DLT solution, DHS expects that the baseline requirements for any such capability SHOULD use *NIST Special Publication 800-130: A Framework for Cryptographic Key Management Systems* as a starting point and that a 'design pattern' and a reference implementation will be made available in a manner that allows for public, transparent and expert review of the security, privacy and cryptographic analysis of the solution.

Analysis and recommendations that support and articulate the trade-offs associated with particular implementation choices are an important aspect of the information sought as part of any proposed solution.

3.3. TTA #3: Decentralized and Derived PIV Credentials

Federal Information Processing Standard (FIPS) 201 originally required a common set of credentials in a smart card form factor, known as the Personal Identity Verification (PIV) Card which is currently used U.S. Federal Government-wide, as intended, for both physical access to government facilities and logical access to Federal information systems.

While the use of the PIV Card for electronic authentication works well with traditional desktop and laptop computers, it is not optimized for mobile devices. In response to the growing use of mobile devices within the Federal government, FIPS 201 was revised to permit the issuance of an additional credential, a Derived PIV Credential (DPC), for which the corresponding private key is stored in a cryptographic module with an alternative form factor to the PIV Card.

Conceptually, a Hardware Digital Wallet under the control of a Holder that contains Decentralized Identifiers and Verifiable Credentials serves the same purpose as a cryptographic module containing a DPC.

This TTA is directly focused on enabling the following outcomes:

- Development of an architecture that allows for a single managed hardware wallet that supports DPCs, Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs)
- Applying Fast Identity Online (FIDO) and W3C Web Authentication (WebAuthN) standards that are standardized ways of performing public-key based authentication in the consumer space to DPC standards and usage.
- Unifying the enrollment and authentication experience across DPC and DID/VCs from an Enterprise Perspective
- Consistent User Experience when using DPCs and DIDs/VCs

Analysis and recommendations that support and articulate the trade-offs associated with particular implementation choices are an important aspect of the information sought as part of any proposed solution.

4. Project Deliverables and Phases

DHS S&T anticipates making phase 1 awards of $50,000 to $200,000 in funding for each award, covering a period of performance of 3 to 6 months. Successful projects will be eligible for subsequent phases of funding with similar levels of funding and duration.

Accordingly, a project receiving 4 phases of funding may receive a total of $200,000 to $800,000

over a total period of performance of 24 months.

Each phase amount cannot exceed $200,000.

At the end of this period, DHS S&T intends that successful projects will have reached a sufficient stage of development for a potential test deployment, or commercial availability to stakeholders, including potential follow on production ordering by DHS. Phase detail is listed in the following chart.

Phase	Funding Level	Deliverables	Due Date
1	$50,000 to $200,000 payable on OTA award	Proof of Concept / Small Scale Demonstration	3–6 months after award
2	$50,000 to $200,000 payable on OTA award	Production and Testing of Working Prototype	3–6 months after successful completion of Phase 1
3	$50,000 to $200,000 payable on OTA award	Deployment of Initial Production Model Prototype Optimization	3–6 months after successful completion of Phase 2
4	$50,000 to $200,000 payable on OTA award	Test & Evaluation, Demonstrations and Commercialization/Transition	Begin after successful completion of Phase 3

Referring to the table above, the required milestones and deliverables for each phase should incorporate the objectives defined as follows:

- **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:
    - 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
    - Articulate a go-to-market commercialization strategy
- **Phase II**: A working prototype with clearly documented APIs, integrated with a multi-factor authentication mechanism that can be reviewed and evaluated. Objectives of this phase are to:

  - Implement the architecture and design to support needed capabilities
  - Ensure that APIs are fully documented and are available for public review
  - Demonstrate the implementation of interoperability specifications within the solution
  - Validate the commercialization strategy with potential customers and partners
- **Phase III**: Production ready prototype able to demonstrate all features and functions of the technology and can be tested in realistic deployment environment that an existing issuer and validator infrastructure. Objectives of this phase are to:
  - Demonstrate a fully functional end to end capability
  - Support the testing and validation of the capability by an independent Red Team
- **Phase IV**: At this phase, technologies would be fully completed designs and reputably provide all proposed features and functionality. Objectives of this phase are to:
  - Deploy the capability in an operationally realistic scenario
  - Incorporate and adjust the capability based on testing and deployment of the capability in an operationally realistic environment

In order to make sure the project is on target and meeting relevant milestones and deliverables, the awardee will provide Monthly Project Status Reports, due at the end of the reporting month. In addition, a telephone conference call will be conducted each month to discuss project status and any issue/concerns/problems, questions that the awardee may have.

5. General Information and Instructions

5.1 Response Dates

Event	Time Due	Date or Date Due
Industry Day(s)	1:00 PM PT*	**December 11, 2018** **SRI International** **333 Ravenswood Ave.** **Menlo Park, CA 94025** **Registration Link:** **https://www.regonline.com/DHS-SVIP-Dec2018**
Applications Due: Applications will be accepted on a continuous, rolling basis. DHS S&T will evaluate applications three (3) times. The deadlines for submitting an application are listed on the right. Applications must be submitted prior to each of the deadlines to be evaluated in the respective review cycle.	12:00 PM PT* (per deadline)	01/11/2019 03/13/2019 05/23/2019
Notification of Application Pre-Oral Presentation Evaluation Results	N/A	Approximately 3-4 weeks following an application deadline
Oral Pitches	N/A	Approximately 4-5 weeks following an application deadline (if requested)
Closing Date/Final Deadline	12:00 PM PT*	**5/23/2019**

* Eastern Time (ET), Pacific Time (PT)

Applications and Application resubmissions received after the closing date/time will not be considered for review.

DHS may decide to close the call early. If this occurs, DHS will publish a notification 30 days prior to closing the call.

5.2 General Instructions

5.2.1 Written applications as described in 5.3 must be received by the deadlines in the following e-mail box: DHS-Silicon-Valley@hq.dhs.gov . Applicants will receive a reply to the application email acknowledging receipt. Any invitations for oral pitches will be coordinated with the applicant and may be conducted by videoconference or in-person.

5.2.2 DHS S&T reserves the right to select for award and to fund all, some, parts, or none of the applications received in response to this OTS solicitation.

5.2.3 The Evaluation Criteria in DHS S&T SVIP 5-Year Innovation OTS (HSHQDC-16-R-B0005) Section 7 "EVALUATION OF APPLICATIONS" applies.

5.3 Application Requirements

5.3.1. To be considered for award, Applicants **MUST** do the following:

- Submit a written **Preventing Forgery & Counterfeiting of Certificates and Licenses application in Adobe PDF format using the application template provided with this call. An architectural Intellectual Property diagram must be included in the application document. The total number of pages including the application and diagram must not exceed 10 pages.** Applications must describe the work proposed for Phase 1, answering the questions as outlined in the **Preventing Forgery & Counterfeiting of Certificates and Licenses Application Form**. Applications should also provide an overview/strategy for the overall effort for Phases 1 through 4. Please note that only content contained in the application will be considered during the review process. No other documents, videos or links to information will be considered. Applicants should be alert for any amendments and changes to this Call.

- Create a user account and register their company in www.sam.gov – This does not need to be done at the application phase but must be done if the applicant is chosen to pitch and provides a successful pitch. The successful applicant must have a registered www.SAM.gov account in order to be awarded and funded.

Applications must be compliant with the aforementioned response dates and other compliance requirements in accordance with the DHS S&T SVIP 5-Year Innovation OTS (HSHQDC-16-R-B0005). Submissions not in compliance will be rejected.

DHS will conduct reviews following each submission deadline and anticipates that reviews will be completed within approximately 3 – 4 weeks following each submission deadline.

The Government may request Applications for other phases and will do so directly with the Company.

5.3.2. The OTS evaluation criteria published in the DHS S&T SVIP 5 Year Innovation OTS (HSHQDC-16-R-B0005) will be utilized for the application evaluation process, and specific to this call, applications will be reviewed for:

- Ability to help DHS operational missions or critical infrastructure facilities;
- Applicability to the DHS use case(s) described;
- Support for standards and specifications to ensure security, privacy and interoperability as detailed in the topic call.
- Overall implementation costs including potential impacts on power requirements, and bandwidth needs;
- Ability to provide secure transmission and storage of collected data;
- Financial soundness of the company, and the business model based on the technology to be supported;
- The scalability and cost-effectiveness of the proposed technology or solution;
- Existing relationships with relevant end users, stakeholders and/or consumers.

5.4. Application Format

See the Preventing Forgery & Counterfeiting of Certificates and Licenses Application posted with this call.

5.5. Pitch Format and Requirements

Applicants invited to present pitches will be limited to **fifteen (15) minutes for their oral presentations**. In addition, applicants making pitches may **provide up to ten (10) slides for presentation in either Microsoft PowerPoint or Adobe PDF**.

5.6 Contractual or Technical Inquiries

All contractual or technical inquiries to this OTS solicitation 70RSAT19R00000002 must be emailed to DHS-Silicon-Valley@hq.dhs.gov. Emails submitting questions are to include **"Questions: Preventing Forgery & Counterfeiting of Certificates and Licenses OTS"** in the subject line. All questions and responses will be posted on the Federal Business Opportunities website http://www.fbo.gov. Questions will only be accepted and answered electronically.

5.7 Order of Precedence

In the event that any of the terms and conditions contained in this OTS solicitation 70RSAT19R00000002 conflict with terms and conditions included in SVIP 5 Year Innovation OTS (HSHQDC-16-R-B0005), the terms and conditions in this OTS call 70RSAT19R00000002 shall take precedence.