U.S. Customs and
Border Protection

Office of Information and Technology

Service Delivery Requirements Document

CBP One

CBP Originating Office: Office of Field Operations

Originating Office POC (Name): (b)(6), (b)(7)(C)

Originating Office POC (Phone Number): (b)(6), (b)(7)(C)

Date of Request: January 6, 2021

Detailed Description of Requirement:

- Compete the integration of CBP ROAM
- Complete the development and implement I-94 Exit
- Complete the development and implement the ability to apply for and update cruising licenses
- Complete the development of the desktop application for air cargo scheduling.
- Complete the development of plugins for easy integration of independently developed capabilities into CBP One.
- Complete the development of the ability to process cargo vessel and aircraft crew members.
- Complete the development of the ability to capture bus travelers and process through mobile primary
- Complete the ability to confirm liveness and biometric matching as plug ins.
- Develop the capability to capture advance information on undocumented individuals who may enter the United States and claim asylum as well as the necessary integration with USEC and Simplified Arrival if appropriate.
- Develop the capability for desktop applications for additional CBP One capabilities
- Complete the development of the ability for air travelers to submit advance information on permitted items along with the necessary officer facing dashboard for managing the notices.
- Develop the ability to schedule all international cargo vessel arrivals along with the necessary officer facing dashboard for managing the arrivals.
- Develop the ability to schedule cargo exams in all environments.

- Develop the capability to apply for and manage Landing Rights Requests along with the necessary officer facing dashboard for managing the request.

- Develop the capability to provide notices of diversions along with the necessary officer facing dashboard for managing the request.

- Develop the capability to provide notices of arrivals for commercial, cargo and private planes along with the necessary officer facing dashboard for managing the request.

Historical Information/Background on Requirement:

CBP One is a mobile application that serves as a single portal to a variety of CBP services. Through a series of guided questions, the app will direct each type of user to the appropriate services based on their needs.

CBP One is available for Android and iOS mobile devices in the Google Play or iTunes mobile application stores. Based on the services/application chosen, there may be a backend component as well, such as the scheduling feature.

Funding Source:

Office of Field Operations agrees to provide the current year and recurring costs for current year and out year funding identified below for the requirement described above. Recurring costs are to be provided at the beginning of the Fiscal Year (October 1, 20XX) by the originating office until such a time that the requirement is cancelled by the originating office and services/items are discontinued or until such time that a permanent adjustment to OIT base budget is made to cover the requirement.

Group	Type	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027
CTO	New Investment	$1,200,000.00	$0.00	$0.00	$0.00	$0.00	$0.00
EDMED	O&M	$0.00	$8,335.00	$10,571.00	$11,995.00	$12,235.00	$12,480.00
EDMED	New Investment	$6,572.00	$0.00	$0.00	$0.00	$0.00	$0.00
CTO	O&M	$0.00	$618,000.00	$636,540.00	$655,636.00	$675,305.00	$695,564.00
	Total	**$1,206,572.00**	**$626,335.00**	**$647,111.00**	**$667,631.00**	**$687,540.00**	**$708,044.00**

Detailed Description of Government Position Cost:

Detailed Description of New Investment Cost (for each FY as applicable):

CTO

Office of Field Operations

Year 1 is for new investment and Year 2-6 are O&M costs for the Year 1 New Investment. In year 1, the new investment cost will be used to enhance the current CBP One application and complete integrations and requirements highlighted under the detailed description portion of this document. This will include integrations such as ROAM, I-94/Exit, cruising license capability, air cargo scheduling, etc. The new investment cost will also include building out the plug-in capability to streamline future integrations.

EDMED

Office of Information Technology

EDMED assumes 2% month over month increase due to natural growth

Detailed Description of O&M Cost (for each FY as applicable):

EDMED

Office of Information Technology

EDMED assumes 2% month over month increase due to natural growth for the out years.

CTO

Office of Field Operations

Year 1 is for new investment and Year 2-6 are O&M costs for the Year 1 New Investment, The O&M costs are only to sustain what will be delivered in Year 1 New Investment . These costs do not include development of new features not outlined in this SDR.

Originating Office Approval:

	Name	Date
Originating Office Signature:	(b)(6), (b)(7)(C) Digitally signed by (b)(6), (b)(7)(C) Date: 2021.06.21 13:15:27 -04'00'	
	Signature	Date

HQ Budget Officer Approval:

	Name	Date
HQ Budget Officer Signature:	(b)(6), (b)(7)(C) Digitally signed by (b)(6), (b)(7)(C) Date: 2021.07.12 14:58:35 -04'00'	
	Signature	Date

Alignment to CBP
Major/non-major investment:

Approval History:

Approver:	Status:	Approved By:	Approval Date:
EDMED	Approved with Budget	(b)(6), (b)(7)(C)	January 14, 2021
ENTSD	Approved without Budget		January 6, 2021
FSD	Approved without Budget		January 6, 2021
CSD	Approved without Budget		January 12, 2021
FMD	No Response - Approved	SDR System User	January 15, 2021
CTO	Approved	(b)(6), (b)(7)(C)	January 26, 2021
DAC	Approved		March 11, 2021

Expiration Date: January 6, 2022

U.S. Customs and Border Protection

Office of Information and Technology
Service Delivery Requirements Document
Southwest Border Operations Support

CBP Originating Office	Office of Field Operations
Originating Office POC (Name)	(b)(6), (b)(7)(C)
Originating Office POC (Phone Number)	(b)(6), (b)(7)(C)
Date of Request	January 18, 2023

Detailed Description of Requirement:

PSPD is supporting Southwest Border Operations by implementing new services, Management Dashboards and Reports of undocumented noncitizens seeking to enter the United States along the Southwest Border (SWB) using the Title 42 Exception processing at the eight ports of entry (Brownsville, Hidalgo, Laredo, Eagle Pass, El Paso, Nogales, San Ysidro, Calexico) by Simplified Arrival Pedestrian (SA PED) primary application. These undocumented noncitizens will be referred for secondary processing. The Arrival and departure information system (ADIS) will ingest the information submitted by these individuals using the CBP One mobile application into its database. This information as well as the encounter information will be shared with USCIS for the individuals processed under this program to start the employment authorization process by ADIS and TDED applications. PSPD Enterprise Reporting team will also provide a dashboard to senior management, leadership, and others with near real time data on the CBP submissions, appointments, and the processing of these undocumented noncitizens. This effort was not included in the FY23 plan for PSPD.

TASPD is supporting Southwest Border Operations by implementing new services and enhancing targeting and vetting systems to process undocumented noncitizens seeking to enter the United States using the Title 42 Exception processing at designated Ports of Entry (Brownsville, Hidalgo, Laredo, Eagle Pass, El Paso, Nogales, San Ysidro, Calexico). Undocumented noncitizens will provide biographic and biometric (facial photo) information to CBP using the CBP One mobile application prior to arrival at a designated Port of Entry. The biographic and biometric (facial photo) information will be sent, processed, and persisted in Unified Passenger (UPAX) and Traveler Verification Service (TVS) for targeting and vetting processes. (b)(7)(E) (b)(7)(E) TVS will create a gallery of the undocumented noncitizens with information submitted by individuals using CBP One mobile and other CBP data holdings. CBP Officers processing undocumented noncitizens upon arrival at the Port of Entry will take an encounter photo of the individual and use TVS (gallery and matching service) to verify the identity of the individual and referral for secondary processing using USEC. (b)(5) (b)(5) (b)(5) The TASPD UPAX, UDR, TVS, and USEC teams are supporting this effort and was not included in the FY23 plan for TASPD.

CTO Office is supporting Southwest Border Operations by implementing updates to the CBP One application's (b)(5)

(b)(5)

(b)(5)

Historical Information/Background on Requirement:

Title 42 is a health policy established in March 2020 by the CDC to stop migrants who were potentially experiencing COVID-19 symptoms from coming across our borders.

The Department of Homeland Security (DHS) prepares for the end of the Title 42 public health order. DHS announced new border enforcement measures to improve border security, limit irregular migration, and create additional safe and orderly processes for people fleeing humanitarian crises to lawfully come to the United States. These measures, taken together, are concrete steps to enhance the security of our border while the Title 42 public health order is in place, and that DHS will continue to build on in preparation for the Title 42 order being lifted.

Funding Source:

Office of Field Operations agrees to provide the current year and recurring costs for current year and out year funding identified below for the requirement described above. Recurring costs are to be provided at the beginning of the Fiscal Year (October 1, 20XX) by the originating office until such a time that the requirement is cancelled by the originating office and services/items are discontinued or until such time that a permanent adjustment to OIT base budget is made to cover the requirement.

Group	Type	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027	FY 2028
PSPD	Gov't Position	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
PSPD	New Investment	$2,000,000.00	$0.00	$0.00	$0.00	$0.00	$0.00
PSPD	O&M	$0.00	$400,000.00	$408,000.00	$416,160.00	$424,483.00	$432,973.00
TASPD	New Investment	$2,000,000.00	$0.00	$0.00	$0.00	$0.00	$0.00
TASPD	O&M	$0.00	$600,000.00	$618,000.00	$636,540.00	$655,636.00	$675,305.00
EDMED	Cloud	$300,000.00	$309,000.00	$318,270.00	$327,818.10	$337,652.64	$347,782.22
CTO	Gov't Position	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
CTO	New Investment	$2,000,000.00	$0.00	$0.00	$0.00	$0.00	$0.00
CTO	O&M	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
ENTSD	New Investment	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	Total	**$6,300,000.00**	**$1,309,000.00**	**$1,344,270.00**	**$1,380,518.10**	**$1,417,771.64**	**$1,456,060.22**

Detailed Description of Government Position Cost:

PSPD

Office of Field Operations

N/A

CTO

Office of Field Operations

N/A

Detailed Description of New Investment Cost (for each FY as applicable):

PSPD

Office of Field Operations

PSPD Investment cost will support Southwest Border Operations by implementing new services, Management Dashboards and Reports of undocumented noncitizens seeking to enter the United States along the Southwest Border (SWB) using the Title 42 Exception processing at the eight ports of entry (Brownsville, Hidalgo, Laredo, Eagle Pass, El Paso, Nogales, San Ysidro, Calexico) by Simplified Arrival Pedestrian (SA PED) primary application. These undocumented noncitizens will be referred for secondary processing. The Arrival and departure information system (ADIS) will ingest the information submitted by these individuals using the CBP One mobile application into its database. This information as well as the encounter information will be shared with USCIS for the individuals processed under this program to start the employment authorization process by ADIS and TDED applications. PSPD Enterprise Reporting team will also provide a dashboard to senior management, leadership, and others with near real time data on the CBP submissions, appointments, and the processing of these undocumented noncitizens.

TASPD

Office of Field Operations

TASPD investment costs will support Southwest Border Operations by implementing new services and enhancing targeting and vetting systems to process undocumented noncitizens seeking to enter the United States using the Title 42 Exception processing at designated Ports of Entry (Brownsville, Hidalgo, Laredo, Eagle Pass, El Paso, Nogales, San Ysidro, Calexico). Undocumented noncitizens will provide biographic and biometric (facial photo) information to CBP using the CBP One mobile application prior to arrival at a designated Port of Entry. The biographic and biometric (facial photo) information will be sent, processed, and persisted in Unified Passenger (UPAX) and Traveler Verification Service (TVS) for targeting and vetting processes. (b)(7)(E) (b)(7)(E) TVS will create a gallery of the undocumented noncitizens with information submitted by individuals using CBP One mobile and other CBP data holdings. CBP Officers processing undocumented noncitizens upon arrival at the Port of Entry will take an encounter photo of the individual and use TVS (gallery and matching service) to verify the identity of the individual and referral for secondary processing using USEC. (b)(5)

(b)(5)

(b)(5) The TASPD UPAX, UDR, TVS, and USEC teams are supporting this effort and was not included in the FY23 plan for TASPD.

CTO

Office of Field Operations

CTO Office is supporting Southwest Border Operations by implementing updates to the CBP One application's (b)(5)

(b)(5)

Detailed Description of O&M Cost (for each FY as applicable):

PSPD

Office of Field Operations

O&M funding will be utilized to fix software bugs, implement security updates and optimize performance.

TASPD

Office of Field Operations

Contractor services to support ongoing operations and maintenance for requirements identified in this SDR. These O&M costs support deployed functionality funded as part of new investment costs identified in this SDR. These costs cover contractor support, patches, bug fixes and standard system maintenance, related CM/security/program control support. These costs cover TASPD requirements defined in this SDR. If additional requirements are identified in the future, a new SDR will be prepared.

CTO

Office of Field Operations

N/A

Originating Office Signature: (b)(6), (b)(7)(C) Digitally signed by (b)(6), (b)(7)(C) Date: 2023.02.09 10:28:39 -05'00'

Signature Date

Originating Office Approval:

Name

HQ Budget Officer Signature: (b)(6), (b)(7)(C) Digitally signed by (b)(6), (b)(7)(C) Date: 2023.02.28 09:50:31 -05'00'

Signature Date

HQ Budget Officer Approval:

Name

Offices Internal Approval:

Signature (Optional) Date

Alignment to CBP
Major/non-major investment: Non-Major Investment

Approval History:

Approver	Status	Approved By	Approval Date
EDMED	Approved with Budget	(b)(6), (b)(7)(C)	January 27, 2023
ENTSD	Approved with Budget		January 27, 2023
FSD	Approved without Budget		January 23, 2023
CSD	Approved without Budget		January 19, 2023
FMD	Approved without Budget		January 19, 2023
CTO	Submitted for Approval		
DAC	Submitted for Approval		
TASPD	Approved with Budget		January 26, 2023

Expiration Date:

PR No. RSSY-23-00071	70RSAT22T00000017
	Modification P00001
	Page 1 of 33

The purpose of this modification to the Department of Homeland Security (DHS) Other Transaction Agreement (OTA) No.70RSAT22T00000017 is to:

(A) Add/fully fund additional within-scope work to increase the number of transactions/sessions being processed under Milestone 2; and

(B) Add Article XV, entitled "*Prohibition on Contracting with Entities using Certain Telecommunications and Video Surveillance Services or Equipment*", to the OT Agreement.

1. This modification is being made pursuant to subparagraph 1 of Paragraph C entitled "Modifications" (Article IV) of the OTA.

2. The above cited changes and other updated information specific to this OTA action are identified in bold, red font.

3. This modification results in an increase of the total funded value of the OTA from **(b)(4)** by **(b)(4)** to $1,869,900.00.

4. Except as modified herein, all the terms and conditions of the OTA remain in full force and effect.

(C) AGREED AND UNDERSTOOD:

iProov Limited	**Department of Homeland Security (DHS)**
By: **(b)(6)**	By: **(b)(6), (b)(7)(C)** Digitally signed by (b)(6), (b)(7)(C) Date: 2023.02.17 14:22:18 -05'00'
Name **(b)(6)**	Name: **(b)(6), (b)(7)(C)**
Title: Chief Executive Officer	Title: Other Transaction Agreement Officer
Date: February 17th 2023	Date:

OTHER TRANSACTION AGREEMENT

BETWEEN

IPROOV LIMITED
10 York Road
London
SE1 7ND, United Kingdom

AND

THE U.S. DEPARTMENT OF HOMELAND SECURITY
Office of Procurement Operations
245 Murray Lane, SW
Washington, DC 20528

CONCERNING:

OTHER TRANSACTION AGREEMENT NO.: 70RSAT22T00000017

EFFECTIVE DATE: Date Executed by Government

PROJECT TITLE/PHASE: RIDIVULB - Remote ID Verification for Use on Land Borders /Phase 5

AUTHORITY: This Other Transaction Agreement is being awarded pursuant to DHS Other Transactions Authority, Section 831 of the Homeland Security Act of 2002, as amended (codified at 6 U.S.C. §391).

DUNS/UNIQUE ENTITY ID (UEI): WKPGFLRZDGK8

TOTAL VALUE OF THE AGREEMENT

Total Estimated Value of the Other Transaction:
Funds Obligated by this Action:
Funds Previously Obligated by OT:

Total Government Funds Obligated to Date by OT:

(b)(4)

PROCUREMENT REQUEST NUMBER: RSSY-22-00157
PROCUREMENT REQUEST NUMBER: RSSY-23-00071

ACCOUNTING AND APPROPRIATION CODES:

R224036-000-R2-67-02-03-000-37-02-0000-00-00-00-00-GE-AP-25-50-000000
R333009-000-N3-67-02-03-000-37-02-0000-00-00-00-00-GE-AP-25-50-000000

TREASURY ACCOUNT SYMBOL:

(b)(4)

TREASURY ACCOUNT SYMBOL:

DHS:
CBP: (b)(4)

This Other Transaction Agreement ("Agreement" or "OTA") is entered between the United States of America ("Government" or "DHS") and iProov Limited ("Recipient") (Collectively, the "Parties").

FOR IPROOV LIMITED

(b)(6)

(b)(6) Chief Executive Officer

February 17th, 2023
Date

FOR THE UNITED STATES OF AMERICA

(b)(6), (b)(7)(C)

Digitally signed by (b)(6), (b)(7)(C)
Date: 2023.02.17 14:23:34 -05'00'

(b)(6), (b)(7)(C) Other Transaction Agreement Officer

Date

ARTICLES		PAGE
ARTICLE I:	AGREEMENT	5
ARTICLE II:	TERM	5
ARTICLE III:	STATEMENT OF WORK	6
ARTICLE IV:	PAYABLE EVENT SCHEDULE AND DELIVERABLES	6
ARTICLE V:	AGREEMENT ADMINISTRATION	12
ARTICLE VI:	OBLIGATION AND PAYMENT	13
ARTICLE VII:	DISPUTES	14
ARTICLE VIII:	RIGHTS OF ACCESS TO INFORMATION AND DATA	16
ARTICLE IX:	CIVIL RIGHTS ACT	22
ARTICLE X:	LIABILITY	22
ARTICLE XI:	SECURITY	23
ARTICLE XII:	GENERAL TERMS AND PROVISIONS	23
ARTICLE XIII:	OPTIONS	26
ARTICLE XIV:	ADDITIONAL TERMS AND CONDITIONS	26
ARTICLE XV:	PROHIBITION ON CONTRACTING WITH ENTITIES USING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT	26

ARTICLE I: AGREEMENT

This Agreement awards iProov Limited a Phase 5 OTA under the DHS/S&T Silicon Valley Innovation Program (SVIP) Other Transaction Solicitation (OTS) HSHQDC-16-R-B0005/ 70RSAT21R00000006, Technical Call No. HSHQDC-16-R-00115- *Enhancing CBP Airport Passenger Processing.*

ARTICLE II: TERM

A. The Term of this Agreement

The period of performance of this fixed price milestone Other Transaction Agreement for Prototype (OTAP) shall be August 19, 2022 through November 18, 2023.

B. Place of Performance

The primary place of performance will be the Recipient's facilities.

C. Termination Provisions

The Government may unilaterally terminate this Agreement fully or partially by providing written notice to the Recipient. This notice will include an effective date of termination as well as instructions for how to stop work. Upon receiving notice of the Government's decision to terminate, the Recipient shall submit a proposal for a termination settlement amount within 30 days of receiving the notice. This proposal shall note which payable milestones have been completed, partially completed, or not started by the Recipient. The Government and the Recipient will negotiate in good faith a reasonable and timely adjustment of all outstanding issues between the Parties as a result of the termination. Failure of the Parties to agree to a reasonable adjustment will be resolved pursuant to Article VII, Disputes. The provisions set forth in Article VII, Disputes; Article VIII, Rights of Access to Information; Article X, Liability; and Article XII, General Terms and Provisions shall survive the termination of this Agreement.

D. Extending the Term

The Parties may extend by mutual written agreement the term of this Agreement if funding availability and research opportunities reasonably warrant. Any extension shall be formalized through modification of the Agreement by the Other Transaction Agreement Officer ("OTAO") and the Recipient.

ARTICLE III: STATEMENT OF WORK

A. Introduction

DHS performs numerous duties at U.S. entry control points. They provide crowd control, inspect baggage and cargo, interview people entering the U.S., review travel documentation, and assist people from many countries while being respectful of multiple cultures and languages. DHS has to manage significant fluctuations in passenger volume depending on airport size, timing of aircraft arrivals, and unforeseen security, weather and/or operational impacts. For example, weather can force an international flight to divert to a smaller airport with smaller DHS infrastructure to handle the passenger load.

DHS is seeking technologies and solutions that would provide DHS/U.S. Customs and Border Protection (CBP) and other components with capabilities to remotely conduct interviews and verify traveler identity. These capabilities would allow DHS to perform all or a portion of required DHS screening procedures without the need for both officer and the traveler to be physically present at the same facility. DHS is interested in technologies that can utilize both DHS infrastructure (booths, video call stations, etc.) and external platforms, such as passengers' own electronic devices, in a secure manner.

B. Background

The iProov solution includes enhancing the functionality of DHS apps to enable members of the *Trusted Traveler* schemes to rapidly and securely cross remote borders without requiring the direct engagement of a DHS Officer in person or online. To deliver this, the technology enables the following primary capabilities:

- Enable travelers to usably capture and send an image of their identity document
- Capture the user's image in a secured way to minimize/eliminate risk of spoofing
- Extract key identification data from the document image by optical character recognition
- Submit the genuine user live image to the DHS/CBP Traveler Verification Service (TVS) database, with identifying document information
- Feedback results to the user

These capabilities are built on iProov's proprietary, patented technology, which captures user imagery and detects spoofs – in the form of replica copies, doctored imagery and replayed recordings- with a uniquely high degree of accuracy without relying on special or trusted hardware. iProov has invented and implemented its Flashmark technology, which uses the screen of the user device to flash a unique, one-time sequence of colors, under server control, onto the user's face. While the user's face is being illuminated by this one-time color code, video of their face is sent to an instance of an iProov server. In the server, the interaction between the screen illumination and the user's face is analyzed. The reflections are analyzed

spatially, using machine learning, to determine if they correspond to those expected from a live, skin-covered living human face. This detects whether a replica (photographic, screen-based, etc.) is being presented. The reflections are also analyzed temporally, to check that the sequence of colors reflected from the user's face corresponds to the one-time code supplied at the beginning of authentication. This detects whether a recording of the user is being presented. These two tests protect the integrity of the captured imagery against the full range of presentation attacks, including those undertaken by compromising the software of the user device.

C. Scope

iProov's Genuine Presence Assurance technology enables organizations to authenticate remote users on their own devices by means of face verification with confidence that the remote user is a real person and present right there, right now. It is highly inclusive, because it can be used on any personal device, irrespective of brand, platform or price, and makes no operative demands on the user. The iProov capability is integrated into existing CBP applications as a Software Development Kit (SDK) to enhance them with the liveness detection feature. The iProov capability is not providing any manner of face matching capability but instead will utilize the existing CBP TVS for that purpose.

The application works with the camera on the user's device to capture an image of the user's face and display an outline sketch of the user. As the user looks into their device, aligning with an oval on the screen, the application illuminates the user's face with a unique sequence of colored light. The application captures a short "selfie" video which is then sent to the iProov liveness detection service. The iProov service will not receive any additional Personally Identifiable Information (PII). The iProov service analyzes the reflected color sequence in the video and confirms the presence of a real, live person. If confirmed as a genuine person, that result is returned to the CBP application. If the result is negative, iProov service provides notification to the app that the liveness detection was a failure.

iProov will evaluate the technology in relevant real-world operational environments with direct end user operation of the system and enhance any current features to meet the CBP use cases. Approximately seven CBP use cases will be considered; however, these use cases fall under one of three capabilities:

- Genuine Presence Assurance with the face matched against an internal database such as TVS
    - Reporting Offsite Arrival- Mobile (ROAM) for small vessel and vehicle remote reporting
    - Cruising license application and port of call processing
    - U.S. Military ship and aircraft processing
    - Commercial cargo crew processing

- Genuine Presence Assurance with the face matched against a digital passport image

(extracted using Near Field Communication (NFC) and cryptographically verified)

  - Trusted Traveler enrollment

- Face verification on fixed or portable tablet with the face matched against a group of prior enrollments

  - Bus passenger processing
  - Remote Port Entry Pilot

iProov shall complete the following for this Phase 5 effort:

- Provide its Genuine Presence Assurance service in accordance with the terms and conditions of this OT Agreement. This service will be delivered at a maximum committed rate of **8 transactions per second**, up to a maximum of **2,400,000 sessions.** A session is a set of transactions that starts with the issue of a token and concludes with the completion of the processing to determine the liveness of a person.

  This increase in throughput (transactions/second) and the increase in the maximum number of transactions are necessary to test and evaluate the throughput and performance of the iProov prototype to meet future CBP mission operations, when this type of liveness detection capability must scale to meet the performance required.

- Collaborate with CBP staff to identify causes of any issues that result in performance levels below 95% pass rate and 1.2 attempts to pass per successful user, and to advise CBP on measures that may be taken to mitigate such issues. iProov does not commit to achieve a specific level of pass rate or numberof attempts to pass, as these may be dependent on factors outside **iProov's** control.

- Assess, with CBP, the feasibility of combining Genuine Presences Assurance with a digital passport image and upon mutual agreement of feasibility, scope of functionality and scale of testing, iProov shall supply a prototype of an app and its associated back-end services for testing by CBP. **Note: The face matching capabilities will continue be the responsibility of CBP, via its TVS capability, while iProov will provide only the liveness detection capability.**

- Assess, with CBP, the feasibility of providing a system for liveness detection on fixed or portable tablets with the face matched against a group of prior enrollments image, and upon mutual agreement of feasibility, scope of functionality and scale of testing, iProov shall supply a prototype of a system and its associated back-end services for testing by CBP. **Note: The face matching capabilities will continue be the responsibility of CBP, via its TVS capability, while iProov will provide only the liveness detection capability.**

Payable Milestones/Deliverables:

Task 1- Kick-Off Meeting and Integration Support

The kick-off meeting will take place via teleconference. The kick-off meeting will be comprehensive in nature. Subsequent support for SDK integration and operation will be provided via email or teleconference

Task 2 – In-Service Operation

Service will be delivered by a production environment to live users and supported by iProov

Milestone 1: Confirmation by iProov of Production Service Availability
Deliverable 1: Credentials permitting CBP to access the production service

Milestone 2: Completion of six months of service
Deliverable 2: Report on prior six months of transaction activity on the CBP production and non-production service instances including number of sessions, distribution of throughput rate and service availability for the period of the test.

Milestone 3: Completion of twelve months of service
Deliverable 4: Report on prior six months of transaction activity on the CBP production and non-production service instances including number of sessions, distribution of throughput rate and service availability for the period of the test.

Milestone 4: Completion of 15 months of service
Deliverable 6: Report on prior three months of transaction activity on the CBP production and non-production service instances including number of sessions, distribution of throughput rate and service availability for the period of the test.

Task 3 – Near Field Communication (NFC) Document and Face Capture

Development and test of a demonstration prototype of an integrated NFC/GPA app and associated service for evaluation to be licensed for small-scale internal test only with an aim of applicability, performance and usability evaluation for a term of 12 months to project end.

Milestone 2: Delivery of integrated NFC/GPA app and non-production service
Deliverable 3: Report describing functionality and use of integrated app for CBP use

Task 4 – Tablet Face Verification

Development and test of a demonstration prototype tablet system applicable to in-person border check verification. Support for collaborative work on assessment of the applicability and specification for live deployment.

Milestone 3: Delivery of demonstration tablet verification system
Deliverable 5: Document describing functionality and use of tablet for test deployment

Task 5 – Feedback Meetings

Meetings to discuss feedback, exchange information and resolve emergent technical problems and issues. These meetings shall take place via teleconference.

Task 6 – Final Assessment Review and Report

Milestone 4: Conduct review meeting, and feedback for Final Report.
Deliverable 7: Report on overall project results in Final Report & Signed attestation of verification data deletion from iProov systems.

Phase 5															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Milestone	M1					M2						M3			M4
Task 1															
Task 2	D1					D2						D4			D6
Task 3						D3									
Task 4												D5			
Task 6															D7

ARTICLE IV: PAYABLE EVENT SCHEDULE AND DELIVERABLES

A. Payment Schedule

The Recipient shall perform the work required by Article III. The Recipient shall be paid for each Payable Milestone accomplished and delivered in accordance with the Schedule of Payable Milestones set forth below. The Schedule of Payable Milestones set forth below may be revised or modified in accordance with subparagraph C of this article.

B. Schedule of Payable Milestones

Cost Per Milestone

Description	Deliverable	Month Completed	Cost Element	Cost per Milestone
Milestone 1 – Service availability				
Provision of production credentials Materials: License for 12 months to iProov production service as specified		**Month 1**	**Labor:**	**(b)(4)**
			Materials:	
			Travel:	
			Total Milestone 1:	
Milestone 2 – Completion of six months of service -Document-based ID verification availability				
Report on prior six months of service		**Month 6**	**Labor:**	**(b)(4)**
Report on functionality and use of integrated app for CBP; report to include throughput, scalability, and performance analysis of the app under the higher throughput levels			**Materials:**	
Materials: ReadID 12-month license for NFC read and verification			**Travel:**	
			Total Milestone 2:	
Milestone 3 -Completion of twelve months of service -Tablet verification availability				
Report on prior six months of service		**Month 12**	**Labor:**	**(b)(4)**
Document on functional use of tablet for test deployment			**Materials:**	
Materials: License for 3 months to iProov production service as specified and Hardware & software for tablet verification system			**Travel:**	
			Total Milestone 3:	
Milestone 4 -Completion of fifteen months of service				
Report on prior three months of service		**Month 15**	**Labor:**	**(b)(4)**
Final report on project results, Signed attestation of verification data deletion from iProov Systems			**Materials:**	
			Travel:	
			Total Milestone 4:	
Total Phase 5 Cost			**Total Labor:**	
			Total Materials:	
			Total Travel:	
			Grand Total:	$1,869,900

C. Modifications

1. At any time during the term of the Agreement, progress or results may indicate that a change in the Statement of Work and/or the Payable Milestones would be beneficial or required to achieve the program objectives. Recommendations for modifications, including justifications to support any changes to the Statement of Work and/or the Payable Milestones, will be documented in a letter and submitted by the Recipient to the Government Program Manager with a copy to the OTAO. This letter will detail the technical, chronological, and financial impact of the proposed modification to the research program. Any resultant modification is subject to mutual agreement of the Parties. The Government is not obligated to pay for nor is Recipient obligated to perform under the additional or revised Payable Milestones until the Payable Milestones Schedule is formally revised by the OTAO and made part of this Agreement. If the revised Schedule of Payable Milestones is not formally revised by the OTAO and made part of this Agreement, then the Recipient may request that the Government terminate this Agreement pursuant to Article II.C.

2. The Government Program Manager shall be responsible for the review and verification of milestone completion, including acceptance of all deliverables due and any recommendations to revise or otherwise modify the Agreement Statement of Work, Schedule of Payments and Payable Milestones, or other proposed changes to the terms and conditions of this Agreement.

3. For minor or administrative Agreement modifications (e.g., changes in the paying office or appropriation data, changes to Government or Recipient personnel identified in the Agreement, etc.), Government may make these types of changes unilaterally and provide Recipient with proper notice of the modification.

4. The OTAO will be responsible for effecting all modifications to this Agreement and providing the Recipient with notice of the modification.

ARTICLE V: AGREEMENT ADMINISTRATION

Administrative and contractual matters under this Agreement shall be referred to the following representatives of the Parties:

Government: (b)(6), (b)(7)(C) Other Transaction Agreement Officer, Tel: (b)(6), (b)(7)(C) E-Mail Address: (b)(6), (b)(7)(C)

Recipient: (b)(6), Chief Executive Officer (CEO), Telephone: (b)(6) E-Mail Address: (b)(6)

Technical matters under this Agreement shall be referred to the following representative:

Government: (b)(6), Other Transaction/Contracting Officer's Representative, Tel: (b)(6)
(b)(6) E-Mail Address: (b)(6)

The Government and the Recipient may change its representatives named in this Article by written notification to the other Party. The Government will effect the change as stated in subparagraph C.4 of Article IV above.

ARTICLE VI: OBLIGATION AND PAYMENT

A. Obligation

The Government's liability to make payments to the Recipient is limited to only those funds obligated under this Agreement or by amendment to the Agreement. The Government may obligate funds to the Agreement incrementally. No legal liability on the part of the Government for any payment may arise for performance under this Agreement unless obligated to this Agreement or until funds are made available to the OTAO for performance and until the Recipient receives notice of availability, to be confirmed in writing by the OTAO. The Recipient is under no obligation to perform work under this Agreement absent funds obligation.

No OTAO or employee of the Government may create or authorize an obligation in excess of the funds available, or in advance of appropriations (Anti-Deficiency Act, 31 U.S.C. 1341), unless otherwise authorized by law.

B. Use of Funds

Federal funds under this Agreement are to be used only for costs that a reasonable and prudent person would incur in carrying out the project and cannot be used for any purposes that are expressly prohibited by law.

C. Payments

1.0 The Recipient shall invoice the Government for each completed milestone per Article IV (B). The following information shall be included on each milestone invoice:

- Agreement Number
- Invoice Number
- A description of services performed
- Quantity of service received or performed
- The time of period covered by the invoice

- Terms of Payment
- Amount claimed

2.0 The Recipient shall document each Payable Milestone by submitting the deliverables in accordance with the Payable Milestone Schedule and Deliverables in Article IV (B). The Recipient shall submit an electronic invoice to the email address below, one (1) copy to the Government Program Manager identified in Article V and one (1) copy to the OTAO for payment approval.

ATTN: S&T Invoices
Burlington Finance Center
P.O. Box 1000
Williston, VT 05495-1000
InvoiceSAT.consolidation@ice.dhs.gov

After written verification and acceptance of the deliverable by the Government Program Manager and approval of the OTAO, the invoice will be forwarded to the payment office within fifteen (15) calendar days of receipt of the invoice. Payments will be made by the Finance Center within fifteen (15) calendar days of the Government accepted and approved invoice. Subject to change only through written Agreement modification, payment shall be made via electronic funds transfer to the Recipient.

3.0 Financial Records and Reports: The Recipient's relevant financial records associated with this Agreement are not subject to examination or audit by the Government, since the confirmed accomplishment of the appropriate milestone completes the obligation of both Parties.

ARTICLE VII: DISPUTES

A. General

The Parties shall communicate with one another in good faith and in a timely and cooperative manner when raising issues under this Article.

B. Dispute Resolution Procedures

1. Any disagreement, claim, or dispute between the Government and the Recipient concerning questions of fact or law arising from or in connection with this Agreement, and, whether or not involving an alleged breach of this Agreement, may only be raised and resolved under the informal administrative procedures outlined in this Article. The

Parties expressly agree to forego the formal dispute resolution procedures available through the Contract Disputes Act, the Tucker Act, the Little Tucker Act, and any other administrative or legal dispute remedies.

2. Whenever disputes, disagreements, or misunderstandings arise, the Parties shall first attempt to resolve the issue(s) through the contracting Points of Contact by discussion and mutual agreement as soon as practicable. In no event shall a dispute, disagreement, or misunderstanding which arose more than three (3) months prior to the notification made under subparagraph B.3 of this Article constitute the basis for relief under this Article unless the Government, in the interests of fairness, waives this requirement.
3. Failing resolution by mutual agreement, the aggrieved Party shall document the dispute, disagreement, or misunderstanding by notifying the other Party in writing (through the OTAO) of the relevant facts, identification of the unresolved issues, and specification of the clarification or remedy sought. Within five (5) working days after providing notice to the other Party, the aggrieved Party may, in writing, request a joint decision by a Government Designee, and a designated Representative of the Recipient ("Recipient Representative"). The other Party shall submit a written position on the matter(s) in dispute within thirty (30) calendar days after being notified that a decision has been requested. The Government Designee and the Recipient Representative shall conduct a review of the matter(s) in dispute and render a decision in writing within thirty (30) calendar days of receipt of such written position. Any such joint decision is final and binding.

4. In the absence of a joint decision, the Parties shall raise any dispute to a higher-level official of the Parties. These officials will review the dispute jointly. Following the review, these officials will resolve, if possible, the issue(s) in writing. Such resolution shall not be subject to further administrative review and, to the extent permitted by law, shall be final and binding.

5. If the Parties are unable to resolve the dispute after all the foregoing steps have been taken, the Parties will seek the input of a mutually agreeable neutral third party and agree to abide by such recommendation.

6. Pending the resolution of any such dispute, work under this Agreement and payments by the Government will continue as elsewhere provided herein, unless the Agreement is terminated by the Government pursuant to Article II(C).

C. Limitation of Damages

Claims for damages of any nature whatsoever pursued under this Agreement shall be limited to direct damages only up to the aggregate amount of DHS funding disbursed as of the time the dispute has risen. In no event shall either Party be liable for claims for consequential, punitive,

special and incidental damages, claims for lost profits, or other indirect damages.

ARTICLE VIII: RIGHTS OF ACCESS TO INFORMATION AND DATA

A. Exchange and Access to of Non-Public Information and Data

During the performance of this OT Agreement, it may be necessary for Recipient to access or for the Parties to exchange information that is not public, i.e. "Nonpublic Information may include but is not limited to, Controlled Unclassified Information ("CUI"), For Official Use Only ("FOUO") information, Personally Identifiable Information ("PII"), or Confidential Commercial Information. If the need arises for Recipient to access any sensitive data requiring safeguarding under Homeland Security Acquisition Regulation (HSAR) class deviation 15-01 or for the parties to exchange such sensitive information under this agreement, additional clauses will be included in Article XI (Security) that outlines the requirements when handling the CUI data that must be addressed prior to exchanging data. The Parties agree that the term "Contractor" in these additional clauses means the "Recipient" of this OT Agreement, including the Recipient's subcontractors.

The Government includes both federal employees as well as other personnel supporting the efforts of the Government, e.g., contractor personnel. Collectively, all information addressed and covered by this Article VIII will be referred to as "Nonpublic Information."

1.0 Definitions.

"Controlled Unclassified Information" or "CUI", means unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulation, and Government/Department wide policy. CUI, and its predecessor designations (e.g., Sensitive But Unclassified or "SBU," For Official Use Only or "FOUO") are addressed in DHS Management Directive MD11042.1 or DHS Instruction 4300A and marked accordingly. CUI includes CUI Specified such as "Security Sensitive Information" (SSI), "Protected Critical Infrastructure Information" (PCII), "Personally Identifiable Information" (PII) or other marking that indicates the information has not been cleared for public release. The Nonpublic Information may be marked when disclosed by the Government to the OT Recipient or marked at a later date as discussed below.

"Confidential Commercial Information" means information that is legally protectable from disclosure and has independent economic value due to it not being "known" or "readily ascertainable." Confidential Commercial Information includes proprietary or business confidential information of the OT Recipient or a third party. Confidential Commercial Information includes information addressed by the Trade Secrets Act (18

U.S.C. §1905).

Example Confidential Commercial Information provided by the Government may include, but is not limited to, information or data associated with limited, restricted, government purpose, or specially negotiated rights as defined by the Federal Acquisition Regulations (FAR) or the Department of Defense supplement to the Federal Acquisition Regulations (DFARS).

Confidential Commercial Information may be marked in a variety of ways that indicate its status. Example markings include proprietary, business proprietary, trade secret or in the case of the FAR, "Limited Rights Notice" or "Restricted Rights Notice." Confidential Commercial Information in general covers proprietary scientific, business, or financial information that an entity (e.g., individual, business, organization) ordinarily would not disclose to the public. Confidential Commercial Information **does not** include the following OTA Recipient information:

i. Information that is publicly known or that is available from public sources;
ii. Information that has been made available by its owner to others without a confidentiality obligation;
iii. Information that is already known by the receiving Party, or information that is independently created or compiled by the receiving Party without reference to or use of the provided information; or
iv. Information that relates to potential hazards or cautionary warnings associated with the production, handling, use or outcomes associated with the work performed under this agreement.

2.0 Nonpublic Information.

Each Party agrees to limit its disclosure of Nonpublic Information to that which is necessary to carry out work under this Agreement, or for Government (noncommercial) purposes, and will place a relevant marking, or notice, on such information (other than PII). In the event that Nonpublic Information is mistakenly shared without proper markings, or is orally or visibly disclosed, the disclosing Party shall make its prompted best efforts to provide the receiving Party written documentation that summarizes such information and describes it as Nonpublic Information with a relevant category (e.g., CUI, FOUO, PII, Confidential Commercial Information, etc.). Each Party has a shared obligation to notify the other Party as soon as possible if in receipt of Nonpublic information that is unmarked or not properly marked to facilitate timely correction of the error and prevent inadvertent or unauthorized disclosure.

Each Party receiving Nonpublic Information agrees to use it only for the purposes described in this Agreement. Either Party may object to the designation of information as Nonpublic Information by the other Party through a written request to the OTAO.

The OTAO shall coordinate all responses of the Parties and take all appropriate actions as related to the Agreement. Failure of the Parties to agree may result in partial or full termination of the Agreement, and any resulting adjustment to the award amount by the OTAO.

2.1 Protection of Nonpublic Information. Nonpublic Information will not be disclosed, copied, reproduced or otherwise made available to any other person or entity apart from that allowed by this Agreement to the extent it does not conflict with controlling law, regulation, government or Department wide policy (e.g., Executive Order) or as otherwise agreed to in writing by the Parties. Disclosure is permitted and there will be no liability where disclosure is required by a court, or administrative body of competent jurisdiction, or federal law or regulation. Each Party agrees to use reasonable efforts to secure all Nonpublic Information other than that which is covered by controlling law, regulation, government/ Department wide policy, or as otherwise provided in this agreement (e.g., CUI, FOUO information) in the same manner that it secures its own Nonpublic Information. If CUI or information categorized under predecessor designations (SBU, FOUO) is provided to a Recipient, DHS Management Directive MD11042.1 will be provided to the Recipient, and a DHS Non-Disclosure Agreement must be signed and returned to the OTAO. The OT Recipient must follow applicable law, regulation, policy in regard to CUI including CUI Specified, its predecessor designations.

3.0 **Flow-down Requirements.** The Parties shall flow down the requirements of this Article to their respective personnel or authorized agents receiving such Nonpublic Information under this Agreement at all tiers.

B. **<u>Publication, Public Disclosure, and Press Releases</u>**

1.0 The OT Recipient shall have the right to publish or otherwise disclose information developed with Government funding, provided that nothing in this provision shall be deemed to authorize disclosure of any information designated by the Government as Nonpublic Information.

2.0 The OT Recipient shall include the following acknowledgment and attribution notice in all non-Governmental publications of information.

Research reported in this [publication/press release] was supported by the Department of Homeland Security, Science and Technology Directorate under Award Number 70RSAT22T00000017. The content is solely the responsibility of the authors and does not necessarily represent the official views of the Department of Homeland Security.

3.0 The OT Recipient shall submit via email a copy of the document to be released to the Program Manager and the Silicon Valley Innovation Program (SVIP) Technical Director at least 30 days prior to the scheduled release date to ensure internal consultation and coordination. The Silicon Valley Innovation Program (SVIP) Technical Director is hereby designated as the reviewing authority for such public releases. The Government will make every effort to respond to the Recipient within 30 days of receipt of the document. If the Recipient has received no response from the Government after 30 days, the Recipient is free to publish the document. However, the **Recipient is strongly encouraged to wait for the Government's response prior to** publication.

C. License

☒ License Not Needed

☐ License Agreement attached

1.0 License Agreement Precedence. Clauses within this OT Agreement will take precedence over any conflicting clauses that exist within any license, Terms of Service (TOS), or similar legal instrument or agreement provided by the OT Recipient.

2.0 Unauthorized Obligations. Any license, Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341) shall be unenforceable against the Government and deemed stricken from the agreement.

3.0 By submitting the deliverables described in Article IV Section B, OT Recipient grants to DHS the following:

(a) 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. This clause supersedes any limiting language that may be included in the reports that contradict the above grant of rights.

(b) Reasonable assistance and additional information concerning Milestones/ Deliverables during the period of performance.

4.0 In the case where the OT Recipient is demonstrating or otherwise sharing work product, related materials, and Know How in connection with this 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) 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.

D. Indemnity

OT Recipient warrants that the intellectual property utilized under this Agreement does not infringe any patent or copyright, does not misappropriate any trade secret of any third party, and does not make use of data in any manner contrary to its authorized usage. OT Recipient indemnifies the Government and its officers, agents, and employees acting for the Government against any liability, including costs and expenses, incurred as the result of the violation of trade secrets, copyrights, or right of privacy or publicity, arising out of the creation, delivery, publication, or use of any data furnished under this contract; or any libelous or other unlawful matter contained in such data.

E. License Rights in Event of Assignments, Acquisition, or Bankruptcy

1.0 Assignment of License Rights

The Government has an interest in ensuring that the rights granted by the OT Recipient in this Article VIII are not eroded or compromised in the event of an assignment. An assignment occurs when the OT Recipient directs a non-party to the OT Agreement to undertake its responsibilities. The OT Recipient shall provide advance notice to the Government, sixty (60) days prior to any assignment, to allow the Government adequate time to evaluate whether the rights granted in this Article VIII can be sustained with the new party.

For clarification, this provision does not impose upon the OT Recipient an affirmative obligation to provide detailed information about its assets or of financial sensitive information about a prospective assignment. However, the OT Recipient must provide information about the specified Deliverables in the OT Agreement and how the Government's Intellectual Property Rights in such Deliverables will be protected. A failure to provide said advance notification shall be considered a material breach of the terms of this Article VIII.

2.0 Acquisition or Merger of OT Recipient's Business

The Government has an interest in ensuring that the rights granted by the OT Recipient in this Article VIII are not eroded or compromised in the event of an acquisition or merger. An acquisition occurs when the OT Recipient's business is acquired in its entirety by a person or organization not a Party to this OT Agreement, or the division or business line which is responsible for the performance of this OT Agreement will be separated or divided from its current ownership. A Merger is when the OT Recipient and any other legal entity combine to

form a new legal entity. The OT Recipient has a duty to safeguard the Government's Intellectual Property Rights in any such acquisition or merger. The OT Recipient shall provide advance notice to the Government, sixty (60) days prior to any such acquisition, separation, or division to allow the Government adequate time to evaluate whether the rights granted in this Article VIII can be sustained under new ownership.

For clarification, this provision does not impose upon the OT Recipient an affirmative obligation to provide detailed information about its assets or of financial sensitive information about a prospective acquisition. However, the OT Recipient must provide information about the specified Deliverables in the OT Agreement and how the Government's Intellectual Property Rights in such Deliverables will be protected. A failure to provide said advance notification shall be considered a material breach of the terms of this Article VIII.

3.0 Bankruptcy or Reorganization of OT Recipient's Business

3.1 The commencement of Chapter 7 liquidation proceeding by the OT Recipient shall be deemed a material breach of the terms of this Article VIII and may result in termination of this OT Agreement. The OT Recipient shall provide advance notice to the Government, ninety (90) days prior to commencing a Chapter 7 liquidation proceeding to allow the Government adequate time to prepare for a dissolution of the OT Recipient's business.

3.2 The Government has an interest in ensuring that the rights granted by the OT Recipient in this Article VIII are not eroded or compromised in the event of Chapter 11 and Chapter 13 Reorganization. The OT Recipient shall provide advance notice to the Government, ninety (90) days prior to commencement of a Chapter 11 or Chapter 13 Reorganization proceeding to allow the Government adequate time to evaluate whether the rights granted in this Article VIII can be sustained after the reorganization.

For clarification, this provision does not impose upon the OT Recipient an affirmative obligation to provide detailed information about its assets or of financial sensitive information about a prospective Chapter 11 or Chapter 13 Reorganization. However, the OT Recipient must provide information about the specified Deliverables in the OT Agreement and how the Government's Intellectual Property Rights in such Deliverables will be protected. A failure to provide said advance notification shall be considered a material breach of the terms of this Article VIII.

F. Information Gleaned by SVIP Participation

To further the goals of SVIP and its OTA recipients, the Government may periodically sponsor information exchange forums where recipients are invited to:

- Demonstrate their product along with that of other recipients;
- **Demonstrate their product's interoperability with the products of other recipients; or**
- Conduct operational testing on Government property or sites.

These forums are for the mutual benefit of the Government and OTA recipients. Recipients are expected to use information obtained from these forums solely to improve their performance as an OTA recipient. These forums are not confidential. Recipients shall refrain from disclosing confidential, proprietary, or trade secret information in these forums. Recipients may not assert intellectual property rights to any information provided by the Government, or to any information provided by other participating OTA recipients in these Government-sponsored forums.

Participation in a forum does not prevent recipients from engaging privately with other participants external to the Government-sponsored forum. In such cases of private engagement, participants are encouraged to protect their own proprietary information through nondisclosure-type agreements. The Government has no role, authority, or responsibility in such private engagements.

ARTICLE IX: CIVIL RIGHTS ACT

This Agreement is subject to the requirements of Title VI of the Civil Rights Act of 1964 as amended (42 U.S.C. 2000-d) relating to nondiscrimination in employment.

ARTICLE X: LIABILITY

A. Property.

Except as otherwise provided in this Agreement or the attached Statement of Work, no Party to this Agreement shall be liable to any other Party for any property that the other Party consumed, damaged, or destroyed in the performance of this Agreement, unless and to the extent it is due to the negligence or willful misconduct of the Party or an employee or agent of the Party. Recipient's liability under this provision is subject to Article XII (C).

B. Other Liability.

The Government shall not be liable to any Party to this Agreement, whether directly or by way of contribution or indemnity, for any claim made by any person or other entity for personal injury or death or for property damage or loss, arising in any way from this Agreement, including, but not limited to, the later use, sale, or other disposition of research and technical developments, whether by resulting products or otherwise, whether made or developed under

this Agreement or contributed by either Party pursuant to this Agreement, except as provided under the Federal Tort Claims Act (28 U.S.C. § 2671 et seq) or other Federal law where sovereign immunity has been waived.

ARTICLE XI: SECURITY

The Parties understand that information and materials provided pursuant to or resulting from this Agreement may be export controlled or unclassified sensitive and protected by law, Executive Order or regulation. Nothing in this Agreement shall be construed to permit any disclosure in violation of those restrictions.

ARTICLE XII: GENERAL TERMS AND PROVISIONS

A. Publicity/Use of Name Endorsement.

The Recipient shall not refer to this agreement in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services. Any public announcement of this Agreement shall be coordinated between the Recipient, the Government, and the public affairs office supporting the Government. By entering into this Agreement, the Government does not directly or indirectly endorse any product or service provided, or to be provided, by Recipient, its successors, assignees, or licensees. The Recipient shall not in any way imply that this Agreement is an endorsement of any such product or service.

B. OT Agreement Officer/Contracting Officer's Representative

a) The OTAO may designate Government personnel to act as the OT Agreement Officer/Contracting Officer's Representative (OTAOR/COR) to perform functions under the OTA, such as review or inspection and acceptance of supplies and services, and other functions of a technical nature. The OTAO will provide a written notice of such designation to the Recipient. The designation letter provided to the OTAOR/COR will set forth the authorities and limitations of the OTAOR/COR under the OTA.

b) The OTAO cannot authorize the OTAOR/COR or any other representative to sign documents, such as OTAs, OTA modifications, etc., that require the signature of the OTAO.

c) The OTAOR/COR for this requirement is (b)(6) Contact information can be found in Article V of this agreement.

C. Governing Law.

The laws applicable to the federal Government shall govern the construction, validity, performance, and effect of this Agreement for all purposes.

D. Waiver of Rights.

Any waiver shall be in writing and provided to all other Parties. Failure to insist upon strict performance of any of the terms and conditions hereof, or failure or delay to exercise any rights provided herein or by law, shall not be deemed a waiver of any rights of any Party hereto.

E. Severability.

The illegality or invalidity of any provision of this Agreement shall not impair, affect, or invalidate the other provisions of this Agreement.

F. Assignment.

Neither this Agreement nor any rights or obligations of any Party hereunder shall be assigned or otherwise transferred by any Party without the prior written consent of the Government. Notwithstanding the foregoing, Recipient, without such consent, shall be permitted to assign this Agreement and all its associated rights and obligations to any U.S. entity that acquires (whether through acquisition, merger, consolidation, reorganization, or otherwise) all or substantially all of the business and assets of such Party to which this Agreement pertains.

G. Corporation Change.

The Recipient shall inform the OTAO and COR within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that will affect the work on this Agreement. The OT will not restrict a company from being acquired (or prevent it from acquiring another firm). **However, an acquisition may result in the Recipient losing its "non-traditional contractor" status, which could impact eligibility for current and subsequent Phase** awards under this and future DHS Other Transaction (OT) Solicitations.

Only the current Recipient may continue performing and invoicing under the current OTA. If the acquisition results in the dissolution of the current Recipient company, the new company must meet Non-traditional Government contractor eligibility requirements (noted below) and receive written consent from the OTAO to continue performing on the current OTA. If the new company does not meet the Non-traditional Government contractor requirements and if the Recipient is unable to continue to perform and invoice under this OTA, the OTA will be terminated by DHS.

Non-traditional Government Contractor, as defined in 10 U.S.C. 2302(9), **means "...an entity**

that is not currently performing and has not performed, for at least the one-year period preceding the selection of sources" by the Government "...any contract or subcontract for the Department of Homeland Security that is subject to **full coverage** under the cost accounting standards pursuant to" 41 U.S.C. 1502. As noted in 41 U.S.C 1502, see CAS 9903.201-2 for types of coverage under the cost accounting standards.

H. Non-US Investment.

During the period of performance of this agreement, the Recipient shall inform the OTAO and COR as soon as possible prior to receiving an investment from a non-US entity. The Recipient shall provide the name of the investment organization, the country of origin, and the amount. This OT will not restrict a company from receiving non-US investments, but changes to the OTA may be required based on the investment information provided by the Recipient, and investments from some entities may affect the recipient's eligibility for OTA continuance.

I. Export Controls.

Nothing in this OTA will be construed as an approval of, certification of, or waiver for an export's compliance with applicable laws and regulations regarding export-controlled items. Each Party maintains the onus for its own due diligence regarding its compliance with export control laws and regulations and remains responsible for conforming to its respective national export control laws and regulations.

J. Entire Agreement.

This Agreement constitutes the entire Agreement between the Parties concerning the subject matter hereof. This Agreement takes precedence over any terms stated elsewhere that may conflict with any terms stated herein. This Agreement may not be amended or modified without a written agreement signed by a duly authorized representative of both of the Parties. This Agreement applies only to the Parties and is not intended to, and does not, create any right, benefit, or trust responsibility, substantive or procedural, enforceable at law or equity, by anybody against the United States or the Recipient, their agencies, officers, or any other person.

K. Follow-on Production Contract or Transaction.

The OTA hereby provides that the Government may issue or award a follow-on production contract or transaction, at the sole discretion of the Government. This possibility is identified in section 2.2.4 of the Department of Homeland Security (DHS), Science & Technology Directorate (S&T), Silicon Valley Innovation Program (SVIP), 5-Year Innovation OTS (70RSAT21R00000006).

ARTICLE XIII: OPTIONS

The Government reserves the right to modify this Agreement on a bilateral basis to include terms and conditions for additional work or to exercise any option for future phases. The cost, technical content, and duration of these additional periods and/or options shall be subject to negotiation between the Parties. The parameters associated with any additional work or options shall be negotiated and agreed to prior to completion of the period of performance of this Agreement. Such optional work is not a new OT award but instead an administrative rescoping and continuation of the original OT award.

ARTICLE XIV: ADDITIONAL TERMS AND CONDITIONS

A. Data Management

1. OT Recipient **production services to DHS** shall be hosted on dedicated servers (bare-metal or cloud-based) in the United States and will not use any compute or storage mechanism outside the USA.

2. OT Recipient, **when providing production services to DHS**, shall not transfer verification data to, or process verification data in any country or territory outside the USA without the prior written consent of DHS

3. OT Recipient **production services to DHS when using non-synthetic data that is being sent to the service from a DHS infrastructure**, shall provide the capability to allow the Government to specify and control how long the data will be retained by the service and when it will be deleted from the service, to meet Government data retention and deletion policies.

    a. This configurable setting provided by the OT Recipient will be configured by **CBP to use its "0-day retention" default setting, which is to automatically** delete the verification data from the OT Recipient service at the end of the liveness detection session.

    b. Any changes to this default setting will require consultation with and agreement from the OTAOR/COR, the SVIP Technical Director and the CBP Program Manager, and will require updates to the PTA/PIA that covers this phase of work.

4. In cases **where DHS infrastructure is transferring and/or sending non-synthetic data to the OT Recipient**, the OT Recipient shall, as part of its final deliverable provide a signed attestation confirming the deletion of all data they may have received either directly or indirectly from DHS during this DHS/SVIP phase of work.

ARTICLE XV: PROHIBITION ON CONTRACTING WITH ENTITIES USING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

Section 889 of the FY 2019 National Defense Authorization Act (NDAA) contains prohibitions related to certain covered telecommunications equipment or services. Section 889 defines **"covered telecommunications equipment or services" as telecommunications and video** surveillance equipment or services produced by Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, or any subsidiary or affiliate of such companies. **The term "Offeror" in this Article means the 'Recipient.**

REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCES SERVICES OR EQUIPMENT

(a) Definitions. As used in this provision—

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition. (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to-

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an

entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(d) Representation. The Offeror represents that-

(1) It □ will, ☒ will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that-

It □ does, ☒ does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) Disclosures.

(1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT IN SOLICITATIONS AND RESULTING CONTRACTS

(a) Definitions. As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data)

received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition. (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications

equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products or commercial services.