

AWARDED ACTIONS FOR ALL VENDORS

Report Date: 02/04/2021

From: 01/01/2017

To: 02/04/2021

Page 1 of 1

Requested by:

Contract#	Order#	Version#	Award Date	Obligated Amount	Simplified Acquisitions	Contract Type	Status	Release Dat
Site: ICE IOSD								
Vendor: 0806010760000 Venntel, Inc								
70CMSD18P00000127			08/07/2018	(b)(4)	Purchase Order		Released	08/07/2018
70CMSD19P00000012			02/15/2019		Purchase Order		Released	02/15/2019
70CMSD20P00000089			06/19/2020		Purchase Order		Released	06/19/2020
70CMSD20P00000159			09/03/2020		Purchase Order		Released	09/03/2020
4 Actions for Vendor 0806010760000 Venntel, Inc				\$270,000.00				
ICE IOSD Site Totals:		4		\$270,000.00				
Grand Totals:		4		\$270,000.00				

PRISM™

■ Documents

Help :: My Profile :: Sign Out


 Quick Open: Create Document:

Search



Document Type

All Awards

Select From

All Awards

Contract/Agreement Number

Order/Call Number

MAS Number

Site

ICE IOSD

☐ Include Related Sites

Vendor/Recipient

venntel

Owner

Buyer

Award Date Range

Begin: End: Status: All

Status Date Range

Begin: End:

Issuing Office

Reconstruct

Both

Description

Search Results

Print Results

Contract/Agreement Number	Order/Call Number	Attachment/Supporting Documents	Line Items	Award Type	Award Date	Buyer	Owner	Site	Issuing Office	Status	Status Date	Vendor/Recipient
70CMSD20P00000159		View Files	View	PO	09/03/2020	(b)(6); (b)(7)(C)		ICE IOSD	ICE/IOSD	Released	09/03/2020	Venntel, Inc
70CMSD20P00000089		View Files	View	PO	06/19/2020			ICE IOSD	ICE/IOSD	Released	06/19/2020	Venntel, Inc
70CMSD19P00000043		View Files	View	PO	01/07/2021			ICE IOSD	70CMSD	Closed	01/08/2021	Venntel, Inc
70CMSD19P00000012		View Files	View	PO	02/15/2019			ICE IOSD	ICE/IOSD	Released	02/15/2019	Venntel, Inc
70CMSD18P00000127		View Files	View	PO	08/07/2018			ICE IOSD	ICE/IOSD	Released	08/07/2018	Venntel, Inc

Line Item Description

Attachments/Support Docs

Clause Number

Project Title

Accounting Code

Recovery Act Funds

Net View

Configure Column Display: 

Market Research

ERO's Alternatives to Detention (ATD) program, participated in a pilot project with the personnel from the Combined Intelligence Unit (CIU); the project's objective was to locate and apprehend ATD Absconders.

The CIU evaluated two of the most commonly accessed geospatial intelligence web-based platforms utilized in support of law enforcement activities, Locate X, sold by Babel Street and Venntel, a subsidiary of location-based marketing company Gravy Analytics.

Services provided by both platforms allow law enforcement personnel to draw a geo-fence around an address or general location, which identifies the latitude and longitude coordinates of multiple mobile devices that were located within the selected area for the timeframe searched.

(b)(7)(E)

(b)(7)(E)

After testing both platforms, the CIU based on all available data concluded that the Venntel platform would significantly increase ERO ATD's efficacy in locating and apprehending ATD absconders.

MEMORANDUM

TO: FILE
FROM: (b)(6); (b)(7)(C) CONTRACT SPECIALIST
SUBJECT: DATA VISUAL PORTAL SEATS
PURCHASE ORDER NO.: 70CTD020P00000016
REQUISITION NO.: 192120ATDOPI20002
SERVICE PROVIDER: VENNTEL, INC.
DATE: 9/8/2020

The U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), Enforcement and Operations Removals (ERO) has data visual portal seats software. Requisition 192120ATDOPI20002 was assigned to the Contract Specialist, (b)(6); (b)(7)(C) in the amount of (b)(4)

Venntel, Inc. quoted an amount of (b)(4) for one year of Data Visual Portal Seats software. A revised quotation was provided on July 23, 2020, to include the optional years for the order. The quote is in-line with the funding provided on the requisition and other [historical] information regarding similar software purchased like this order.

(b)(7)(E)
(b)(7)(E)
(b)(7)(E)
(b)(7)(E)
Venntel, Inc. is the only provider that could provide the has data visual portal seats software licenses with the specifications that ERO requires. The following is a breakdown of the Base Year and Option Years:

Base Year: licenses x (b)(4) / year = (b)(4)
Option I: licenses x \$(b)(4) / year = (b)(4)
Option II: licenses x (b)(4) / year = (b)(4)
Option III: licenses x (b)(4) / year = (b)(4)
Option IV: licenses x (b)(4) / year = (b)(4)

(b)(7)(E)
Total Purchase Order Value: \$200,000.00

PROCUREMENT AWARD SUMMARY

70CTD020P00000016

BASE

Based on similar and historical information, I, the Contract Specialist, have determine the prices of the Purchase Order and the Option Periods are be fair and reasonable, and I support the award for this Purchase Order and the Option Periods being made to Venntel, Inc.

Based on the above-mentioned information, it is recommended that Purchase Order, 70CTD020P00000016, be awarded to Venntel, Inc. in the amount of (b)(4) This award represents a technically acceptable solution that is fair and reasonable.

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Contract Specialist

DHS/ICE/OAQ/ITD

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Contracting Officer

DHS/ICE/OAQ/ITD



A NEW WAY TO SIGN IN - If you already have a SAM account, use your **SAM email** for login.gov.

[Log In](#)

[Login.gov FAQs](#)

⚠️ ALERT: SBA connectivity is experiencing an outage. For questions about small business size status, users should return later or contact SBA directly (www.sba.gov).

⚠️ ALERT: SAM.gov will be down for scheduled maintenance Saturday, 09/12/2020 from 8:00 AM to 1:00 PM.

Entity Dashboard

Venntel, Inc.
DUNS: 080601076 CAGE Code: 7UV15
Status: Active
Expiration Date: 08/03/2021
Purpose of Registration: All Awards

2201 Cooperative Way Ste 600
Herndon, VA, 20171-3005 ,
UNITED STATES

▸ [Entity Overview](#)

▸ [Entity Registration](#)

▸ [Core Data](#)

▸ [Assertions](#)

▸ [Reps & Certs](#)

▸ [POCs](#)

▸ [Exclusions](#)

▸ [Active Exclusions](#)

▸ [Inactive Exclusions](#)

▸ [Excluded Family Members](#)

[RETURN TO SEARCH](#)

Entity Overview

Entity Registration Summary

Name: Venntel, Inc.
Business Type: Business or Organization
Last Updated By: (b)(6); (b)(7)(C)
Registration Status: Active
Activation Date: 08/03/2020
Expiration Date: 08/03/2021

Exclusion Summary

Active Exclusion Records? No



IBM-P-20200814-1154
WWW1

[Search Records](#) [Disclaimers](#) [FAPIS.gov](#)
[Data Access](#) [Accessibility](#) [GSA.gov/IAE](#)
[Check Status](#) [Privacy Policy](#) [GSA.gov](#)
[About](#) [USA.gov](#)
[Help](#)

This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.



U.S. Immigration
and Customs
Enforcement

STATEMENT OF WORK

Geolocation Data Subscription Service

MARCH 23, 2020

Enforcement and Removal Operations

Immigration and Customs Enforcement

STATEMENT OF WORK (SOW) FOR GEOLOCATION DATA SUBSCRIPTION SERVICE

1.0 GENERAL

Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO) has a complex and targeted public safety mission to collect and act upon timely and accurate information relating to the enforcement of immigration laws within the U.S. ERO also maintains a role in continuity of operations, emergency response, and crisis management to include establishing and maintaining an agency-wide secure data communication connectivity.

1.1 BACKGROUND

ERO has a responsibility for identifying and exploiting emerging data from traditional and non-traditional sources which can significantly enhance the capability of furthering ICE's mission. ICE personnel conduct research on readily available public domain open source information and investigate known and illusive criminal elements to mitigate violations of U.S. immigration law. Geolocation data service is a data subscription that will give ICE ERO the capability to view location signals from known locations of interest and track movement to identify patterns and reveal other source locations. It is a tool that will greatly enhance law enforcement abilities for identifying administrative and criminal activity as well as effective operational decision-making.

ERO must remain diligent in seeking new and improved means of combatting the challenges that face our law enforcers for identifying, tracking, investigating, and apprehending those who violate criminal and administrative law. Geolocation data adds to ERO's ability to successfully meet those mission goals and their public responsibility by leveraging geospatial movement patterns into a given timeline.

1.2 SCOPE

The purpose of this Statement of Work (SOW) is for a contractor to provide ICE ERO with access to their host server through the ICE firewall for a geolocation data subscription service, without the need for additional hardware, middleware or software installation. The geolocation service must be web-based whereas no data will reside within ERO IRMnet.

1.3 OBJECTIVE

This requirement is for access to global mobile location database via the web to support ICE users. The contractor will allow access to their host server through a subscription service which requires no ICE infrastructure changes.

The Government's requirement is that the data allows ERO to accurately identify digital devices within the U.S. and international borders for information on a specific location, or a designated polygon area, during a specified time period within the preceding years, greater than two (2) years.

The Government has the requirement to ensure the integrity of the information to include:

- Removing fake, spoofed and fraudulent signals
- Reduction of signal redundancies, exceptions and noise
- Combining multiple data sources into a unified data stream

The Government has a requirement for geospatial and metadata algorithms with machine learning capabilities to process and provide data to a user via analytics enabled web portal. The analytic tools will include at a minimum polygonal searches and time/location search.

The Government has a requirement for the data to be timestamped with latitude, longitude and horizontal accuracy.

The Government has a requirement that data can be collected from the highest number of sources available, (b)(7)(E)

(b)(7)(E)

The Government has a requirement that the database has the capability to save specified polygon searches for future analysis applications.

The Government has a requirement to that the database has the capability to save specified date ranges as a default.

(b)(7)(E)

(b)(7)(E)

The Government has a requirement for a minimum of (b)(7)(E) licenses with the ability to add additional licenses throughout the duration of the contract period to a maximum of licenses.

This requirement is for:

Nomenclature	Agency	Base POP Start	Base POP End	Number Licenses
Geolocation Data Service	ERO	09/11/2020	09/10/2021	(b)(7)(E)

The Government has a requirement to protect Personally Identifiable Information (PII) so the commercial location data sources must not contain PII and is provided with the permission of the individual.

The Government has a requirement for training and technical phone support to maximize user efficiency in understanding and utilization of the database.

The Government has a requirement for account management to include, but not limited to, the ability to transfer accounts upon government request, to ensure maximize usage of licenses.

(b)(7)(E)

The Government has a requirement that each user has access to two (2) hours of vendor provided training per named user on the analytic capabilities within the web portal and understanding of the data source.

1.4 APPLICABLE DOCUMENTS

None

2.0 PERIOD OF PERFORMANCE

The period of performance (POP) will be for one (1) base year and four (4) option years.

POP Type	POP Start Date	POP End Date
Base Year	09/11/2020	09/10/2021
Option Year1	09/11/2021	09/10/2022
Option Year2	09/11/2022	09/10/2023
Option Year3	09/11/2023	09/10/2024
Option Year4	09/11/2024	09/10/2025

2.1 PLACE OF PERFORMANCE

ICE / ERO

2.2 INTELLECTUAL PROPERTY

The General Law Attorney will involve a DHS Intellectual Property Attorney, as needed.

2.3 AUDIT LOGS & REPORTS

Audit logs/reports will be provided to the Government Program Manager (PM) upon request to ensure appropriate use of the service.

The COR will work with the vendor to develop a splash screen that identifies appropriate use cases for the service. The Government will require users to agree to ICE’s use terms prior to initiating queries for geolocation data.

2.4 SECTIONS 508 COMPLIANCE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the “Electronic and Information Technology Accessibility Standards” set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the “Access Board”) in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at <http://www.access-board.gov/> or at <http://www.section508.gov>.

3.0 GOVERNMENT TERMS & DEFINITIONS

ACRONYM LIST

COR	Contracting Officer Representative
ERO	Enforcement Removal Operations
ICE	Immigration and Customs Enforcement
PII	Personally Identifiable Information
PM	Program Manager
POP	Period of Performance
SOW	Statement of Work

4.0 GOVERNMENT FURNISHED RESOURCES

The Government will not furnish any resources to the contractor in support of this contract.

5.0 GOVERNMENT ACCEPTANCE PERIOD

The COR will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance.

Deliverables

Item	SOW Reference	Deliverables	Frequency	Distribution
1	Section 1.2, 1.3	Geolocation License	Upon Request	ICE users
2	Section 1.3	New User Training	Upon Request	ICE users
3	Section 1.3	Technical Phone Support	As Needed	ICE users
4	Section 2.3	Audit Reports	Upon Request	PM

Acceptance by the Government of satisfactory products/services will be made once all the terms and conditions of the contract are fulfilled.

The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

The COR will work with the vendor to develop a splash screen that identifies appropriate use cases for the service. The Government will require users to agree to ICE's terms of use prior to initiating queries for geolocation data and will follow up with Privacy once this requirement has been addressed.

Form G-514

REQUISITION - MATERIALS-SUPPLIES-EQUIPMENT

Activity Symbols
ATTACHMENT A

REQUISITION NUMBER: 192120ATDOPI20002

Item No.	Contract No.	Task Ord No.	Project	Task	Fund	Program	Organization	Object	UDF	Amount
1			NONE000	000	E4	36-42-00-000	18-06-0300-40-10-00-00	GE-25-14-00	000000	\$40,000.00

APPROPRIATION SYMBOL CROSSWALK:

FUND	FY	TAS	TITLE	AMOUNT
E4	2020	7000540		40,000.00

CONTRACT ACTION REVIEW (CAR)

DATE SUBMITTED	CONTRACT/ORDER NO.	LIST <u>ANY</u> SUPPORTING DOCUMENTS THAT SHOULD BE UPLOADED IN THE FILE PER THIS ACTION <u>AND</u> ARE NOT SPECIFIED ON THE FILE CHECKLIST
08/11/20	70CTD020P000000016	
MODIFICATION #	RFQ/RFP NO.	
-	-	

FIRST LEVEL REVIEWER COMMENTS	CONTRACT SPECIALIST COMMENT RESOLUTION

SECOND LEVEL REVIEWER COMMENTS	CONTRACT SPECIALIST COMMENT RESOLUTION

LEVEL ONE REVIEWER <i>(Printed name and position):</i>	<div style="border: 1px solid black; height: 20px; width: 90%;"></div>
LEVEL TWO REVIEWER <i>(Printed name) * Required if > \$500,000:</i>	
CONTRACT SPECIALIST <i>(Typed/printed name):</i>	<div style="border: 1px solid black; height: 20px; width: 60%;"></div>

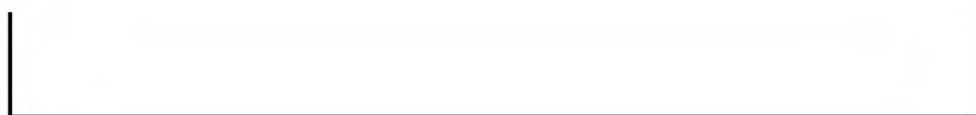
*Indicates for ITD use only

(b)(7)(E)

Totals:	\$40,000.00	\$0.00	\$40,000.00	<< Current Total Obligation
----------------	-------------	--------	-------------	-----------------------------

Date _____

Award	1st Level Reviewer
Review	2nd Level Reviewer



LEGEND: OAQ MS CONTRACT & MODIFICATION LOG

Field	Description	Example
*If associated with a MAOL program, add program level:	Field is for ITD use only. Select from the dropdown menu the priority level of the MAOL program	1
*Additional Originating Offices:	Field is for ITD use only. If there are multiple Originating Offices, please insert all that apply (if applicable)	CIO, HSI, OPLA
Actual Close Date:	The date a contract was closed out in PRISM; this will be left blank until the closeout is completed Enter a date in MM/DD/YYYY format	9/17/2015
Base / Mod #:	Indicate the base or modification # that corresponds to the subsequent cells in the row	Base P00005
Base / Mod Date:	Enter the effective date of base agreement or the effective date of the modification Enter a date in MM/DD/YYYY format	8/9/2014
Contract Clause -8:	Select from the dropdown menu to indicate if the -8 clause has been evaluated and included in the contract	Evaluated at Award
Contract Number:	Enter base contract or agreement number of how it is entered in PRISM	HSCEMS-13-A-00000
Contract Specialist:	Enter the name of the current CS	(b)(6); (b)(7)(C)
Contract Type:	Select from the dropdown menu to indicate the contract type	Agreement FFP
Contract Vehicle:	Select from the dropdown menu the most appropriate contract vehicle based on the products and services offered	EAGLE II FSSI
Contracting Officer:	Enter the name of the current CO	(b)(6); (b)(7)(C)
Cumulative \$ Amount of Mod Changes:	Cumulative amount of the modification (mod) changes Field is updated automatically	<i>*This field is automatically calculated. Do not enter any data.</i>
Cumulative \$ Amount of Total Obligation:	Cumulative amount of the total obligation Field is updated automatically	<i>*This field is automatically calculated. Do not enter any data.</i>
Current Max Ceiling Amount:	Field is updated automatically to only display the most current maximum ceiling amount	<i>*This field is automatically calculated. Do not enter any data.</i>
Current Option Period:	Include the current option period that the contract is in at the time of the log update; Enter N/A if option periods do not apply	2 of 4 (indicates that we are in option period 2 out of 4)
Description of Supply / Service:	Provide a description of the contract and include the program name (as applicable)	EEO Investigation Services
Dollar Amount Increase / (-) Decrease:	Enter the modification amount (do not include the \$ sign); type a minus (-) sign in front to indicate a decreased modification amount A zero (0) MUST be entered to enable ULO calculations Enter a zero for \$0 modifications	<i>Dollar Amount Increase:</i> (b)(4) <i>Dollar Amount Decrease:</i> (b)(4)
File Reviewer Last Name:	Insert the reviewer's last name after reviewing Q: drive documentation	(b)(6); (b)(7)(C)
Final POP End Date (all options exercised):	Indicate the final POP end date that is specified once all option periods are exercised according to the contract/agreement Enter a date in MM/DD/YY format	4/15/2019
Total Value or Maximum Ceiling Amount:	Enter in the maximum ceiling amount as it changes or Enter in the total value for multi-year contracts	(b)(4)
Notice of Intent Date:	Date that OAQ sends notice of intent to exercise an option period Enter a date in MM/DD/YYYY format	6/30/2016 <i>* Enter a date. Please do not indicate "30 days after POP ends"</i>
Obligated Amounts: Base Award Modifications	Enter in dollar amounts for "Base Award" and "Modifications" sections; formulas are in the spreadsheet for easy calculations	(b)(4)
Order Number:	Enter delivery or task order number of how it is entered in PRISM	HSCEMS-16-F-00000 HSCEMS-14-F-00000

Order Type:	Select from the dropdown menu to indicate the order type	IDIQ BPA DO/TO
Originating Office:	The office that requested the service or supply	M&A - ODCR HSI
POP End Date:	Enter a date in MM/DD/YYYY format	3/31/2019
POP Start Date:	Enter a date in MM/DD/YYYY format	4/1/2014
Program Contact:	Enter the name of the COR	(b)(6); (b)(7)(C)
Program Name:	Enter the name of the program completing the service	TECS Modernization SEVIS II
Projected Close Date:	Date the agreement can be closed out in PRISM after the waiting period for invoices, etc. (this is not the actual close date) Enter a date in MM/DD/YYYY format	1/31/2017 * Enter a date. Please do not indicate "60 days after POP ends"
Purpose (be descriptive):	Provide a brief description of the purpose and type of modification made in this column Detail in this column is important for future reference to understand the details of the modification	Extending the funded POP through 8/31/2016 Changed the COR from (b)(6); (b)(7)(C) to (b)(6); (b)(7)(C) * Do not simply indicate "funding only" or "admin mod"
Sub-Contractor (as applicable):	If applicable, enter the subcontractor's name along with the available contact information for the main POC	XYZ Company (b)(6); (b)(7)(C)
Telephone #:	Enter the phone number of the current CO	202-732 (b)(6);
Telephone #:	Enter the phone number of the current CS	202-732 (b)(7)(C)
Telephone #:	Enter the phone number of the current COR	202-555
Total:	Dollar amount will calculate automatically based on the base award and modifications totals	*This field is automatically calculated. Do not enter any data.
Vendor / Service Provider:	Enter the name of the contractor or service provider for the contract or agreement. In the event a BPA contract has multiple vendors, enter in "Multiple Vendors"	ABC Company Multiple Vendors
Vendor Contact Information:	Enter the vendor's primary POC name, email address or phone number	(b)(6); (b)(7)(C) @abc.com or 555-555-1212
Vendor Socio-Economic Status:	Enter the vendor's business classification. If a vendor has multiple classifications, type all that apply	8A Small, Women-Owned



**U.S. Immigration
and Customs
Enforcement**

9/9/2020

Contracting Officer's Representative (COR) Appointment Letter

Subject: Appointment as a COR

From: (b)(6); (b)(7)(C)

To:

You are hereby appointed as the COR under 70CTD020P00000016 with Venntel, Inc for Data Visualization Portal Seats Licenses. The Contracting Officer will rely on you as a technical expert to provide advice regarding the quality and timeliness of the work performed. As the COR, your primary duties include assisting the Contracting Officer with monitoring the prime contractor's performance; ensuring that all technical requirements under the contract are met; timely delivery of products or services by the delivery date or within the period of performance; and at the price or within the estimated cost stipulated in the contract. The duties or authorities in this letter are not delegable; therefore, you must advise the Contracting Officer, (b)(6); (b)(7)(C) or the Contract Administrator/Specialist (b)(6); (b)(7)(C) immediately when you are unable to perform these duties.

Scope of Authority

COR Responsibilities and Duties

Your duties, as applicable to the contract, are as follows:

I. Performing surveillance/inspection and acceptance, as listed in HSAM-Appendix W, Exhibit 1.

- A) Perform on-site surveillance in accordance with the surveillance plan. Document surveillance activities and provide a copy of documentation to the contracting officer. Review technical proficiency and compliance against the technical provisions of the contract and verify the performance of work by the contractor.
- B) Perform surveillance of the performance under the business agreement and conduct inspections necessary to assure performance and compliance with the terms and conditions of the agreement.

- C) Assure prompt review of draft reports and approval of final reports to contractor to assist with meeting the specified completion date of the contract, and assuring prompt inspection and acceptance, or rejection, of deliverable.
- D) Notify the Contractor of deficiencies observed during surveillance. Record and report to the contracting officer all incidents of faulty or nonconforming work, delays, or problems that may disrupt or hinder future performance.

II. Monitoring activities, cost (see HSAM 3016.601, 3032.7000, and 3042.1500), providing input to contractor performance evaluations and notifications to the Contracting Officer (see examples):

- A) See HSAM 3016.601 and 3032.7000 for specific requirement in monitoring cost reimbursement contracts & time-and-material and labor hour contracts.
- B) For T&M and labor-hour contracts, the COR duties for monitoring contract performance should include, at a minimum, verifying:
 - 1) The work performed is consistent and conforms with the Statement of Work (SOW), Statement of Objectives (SOO), or Performance Work Statement (PWS);
 - 2) The appropriateness of the categories of labor used;
 - 3) The reasonableness of the number of hours worked, including any approved overtime;
 - 4) The reasonableness of materials used; and
 - 5) The hours worked against the hours billed for the invoice period.
 Note, see HSAM Appendix S for a “Payment Approval Template.”
- C) For contracts awarded after August 2011 with a dollar value over \$500,000 for supplies and \$1,000,000 for services, enter the contractor performance evaluation information into Contractor Performance Assessment Reporting System (CPARS). Component Head of the Contracting Activity (HCA) are responsible for contractor performance evaluations procedures and policies (see HSAM 3042.1500) for ensuring that contractor performance evaluations (interim and final) are included in the Past Performance Information Retrieval System (PPIRS) through the CPARS. The CO’s identification and requested assistance from the COR for input into the contractor evaluations can be efficiently assigned via the appointment COR letter. For access to CPARS, see Section IX, Training.

III. Notification examples:

- 1) Any requests for changes from a contractor.
- 2) Potential labor disputes or workforce problems.
- 3) Lack of performance that may jeopardize the cost or required schedule.
- 4) Monitoring financial management controls with respect to the allocation of appropriated dollars under the designated contract.
- 5) Possible changes in contractor management and/or key personnel.
- 6) Disagreements with the contractor regarding performance of SOW/SOO requirements or other potential disputes with the contractor about technical or other business matters.
- 7) Any possible contractor deficiencies or questionable practices, so that corrections can be made before problems become significant.

- 8) Procurement fraud, waste, abuse, bribery, conflict of interest, or other improper conduct to the CO and agency office, such as the Office of Inspector General (OIG).
- 9) All problems, potential disagreements, or controversy, both oral and in writing, regarding the status of the contract and performance of its requirements.

IV. Making recommendations for invoices and payments (See HSAM 3016.601 and 3032.7000.)

- A) Report any discrepancies in payment vouchers to the CO. Provide documentation to support the representation.
- B) Evaluate progress payment requests based on costs incurred and actual work accomplished.
- C) Certify invoices to the contracting officer for payment, using the electronic invoicing system in FileOnQ – WebView. For Web View training, please visit [OFM website](#).
- D) Reviewing contractor invoices for accuracy of work completed in accordance with contract requirements and certify acceptance or rejection.
- E) Review the contractor's invoices/vouchers for reasonableness and applicability to the contract and recommend to the CO approval, conditional approval, or disapproval for payment. The review must be completed within five days after receipt of the invoice or voucher. If you cannot meet the required review time, advise the CO or contract specialist so that action can be taken to ensure Government compliance with the Prompt Payment Act, thereby avoiding the payment of interest penalties to the contractor.
- F) Review the contractor's invoices/vouchers to ensure that they accurately reflect the work completed in accordance with the requirements of the contract, and certify or reject acceptance of the delivered items. Submit certified invoices/vouchers to the Dallas Finance Center and copies to the CO in a timely manner.
- G) See HSAM 3106.601 and 3032.7000 requirements for processing payment for cost reimbursement and time-and-material and labor hour contracts.

V. Managing Government Furnished Property (used when Government property is specified in the contract).

	YES	NO
Government Furnished Property (GFP)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Government Furnished Equipment (GFE)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- A) You are not authorized to provide any Government-owned (or leased) equipment or supplies or use of Government space to the contractor, other than those specifically identified in the contract and authorized by the Contracting Officer.
- B) If applicable, ensure Government Furnished Property and/or Equipment is made available in a timely manner.
- C) Request the Contracting Officer authorize Government furnished property/equipment, and when requested by the Contracting Officer, provide disposition advice on Government-furnished property/equipment or contractor-acquired property.

VI. Managing Contractor Employee Access and Security through established application process for cards, badges, or credentials (when security requirements are specified in the contract). Exit Checklist MUST be used when contractors leave a contract, move/transfer to a new contract, or is terminated (Click for [Attachment A](#)).

Serves as a Federal sponsor for contractor, by assisting with the agency Security process, to include handling, as appropriate, the Contractor Suitability worksheet for contractor requiring a DHS PIV card, notification of results of the contractor access submissions, ensuring the return of the DHSPIV card, and communication of contractor and employee's changes in status.

VII. Preform oversight of inherently Governmental and critical functions. See HSAM 3007.5 and DHS Guide on Inherently Governmental and Critical Functions regarding specific requirements:

Perform on-going reviews of the functions performed by contractors, especially how work is performed and the manner in which Government personnel are managing services acquisitions. Reviews should focus on functions that are closely associated with inherently governmental functions and critical functions. In addition, monitor contracts to ensure that the relationships between Government personnel and contractors have not evolved into unauthorized personal services or inherently governmental functions. Also, provide information to the CO so the CO can document the contract file to reflect the results of the on-going review.

VIII. Non-Delegable Functions and Exclusions (See HSAM-Appendix W, Exhibit 2 for requirements & HSAM3042.270-3(b)(2)).

As COR you shall not:

- A) Contracting officers may not delegate to the COR the following authorities or activities:
- B) To make or give the appearance of being able to make commitments, modifications, or other actions which would commit the Government to a change in contract price, performance, quality, quantity, or the delivery schedule.
- C) To provide guidance to the contractor, either orally or in writing, which might be interpreted as a change in the scope or terms of the contract.
- D) To change or modify any of the terms and conditions, or statement of work of a contract or business agreement.
- E) To take any action with respect to termination, except to notify the contracting officer that action may be necessary and to assist with the process as requested.
- F) To engage in conduct prejudicial to the Government.
- G) To sign contracts or contract modifications.
- H) To solicit proposals.
- I) To direct a contractor (oral or written) to begin work prior to contract award date or notice to proceed, or to stop work.
- J) To participate in negotiations with a contractor outside of the presence of a contracting officer.
- K) To render a decision on any dispute or question of fact under the Disputes clause of the contract.
- L) To interfere with the contractor's management by supervising contractor employees or otherwise directing their work efforts.

- M) To specify limitations and include the admonition that the COR may be personally liable for unauthorized commitments.
- N) To make any agreement with the contractor relating to the expenditure of Government funds.

IX. FAR and DHS Authorities/Directives, Government Ethics, and Training: (See HSAM 3042.270-3(b)(3)).

Adherence to applicable requirements for ethics (annual training), procurement integrity, no conflict of interest, and proper standards of conduct, including the identification of regulations (e.g., FAR Part 3, Improper Business Practices and Personal Conflicts of Interests), statutes, or agency directives governing these topics (e.g., 5 CFR Part 2635 Standards of Conduct and Management Directive 0480.1, Ethics/Standards of Conduct (or any successor directive)).

Complete and file with the ICE Ethics Office an OGE-450 (Confidential Financial Disclosure Report), via the appropriate confidential report system. Forward your completed OGE-450 as required electronically to the ICE Ethics Office (Office of the Principal Legal Advisor (OPLA)). In addition, you are required to complete annual ethics training as stipulated by the ICE Ethics Official. More information can be found at the [ICE Ethics Intranet Site](#).

Use of authority for appointment letter is “Pursuant to the Federal Acquisition Regulation (FAR), the Homeland Security Acquisition Regulation (HSAR), you are appointed the COR or Alternate COR.”

Training:

Adherence to DHS Annual Skills Currency to maintain COR certification and any other special instructions for obtaining training, to include annual ethics training or other relevant training, as listed in HSAM Appendix W.

(b)(6); (b)(7)(C) In order to obtain access into the CPARS, you are required by ICE/OAQ to take the following courses (CPARS Overview and Quality and Narrative Writing) that are available through the CPARS website (links below). Please contact the ICE Point of Contact, (b)(6); (b)(7)(C) via phone: (202) 732- or email: (b)(7)(E)@ice.dhs.gov or (b)(6); (b)(7)(C)@ice.dhs.gov for questions or assistance.

CPARS Overview (2.25 hours). **Take Training** – This training will give the student an overview of the policies and regulations governing CPARS, the CPARS Workflow, and CPARS Application functionality. Taking the CPARS Overview is a prerequisite to Quality and Narrative Writing and Focal Point Functions.

Quality and Narrative Writing (1.75 hours). **Take Training** – This training will give the student an understanding of the need for quality and accuracy in narrative writing, examples of narratives and resources to aid in creating quality Past Performance Evaluations, and examples of strategies for making the CPARS-FAPIIS process more effective. Taking the CPARS Overview is a prerequisite to taking this class.

Federal Acquisition Certification Requirements.

Based on the technical and administrative characteristics of this contract, I have determined that the COR must possess a Federal Acquisition Certification (FAC) level II. Your appointment as COR is based on the training, experience, certification, and other qualifications cited in your nomination letter. It is your responsibility to maintain your certification and/or qualifications for COR on this contract, including completing continuous learning points. If you fail to maintain your FAC COR certification at this level, DHS is prohibited by law from paying you for performing COR functions.

Please contact the ICE/OAQ Point of Contact: (b)(6); (b)(7)(C) via phone: (202) 732-(b)(6); (b)(7)(C) or email: (b)(6); (b)(7)(C)@ice.dhs.gov for COR/FAC certification/training questions.

As COR you shall be aware of the following:

Federal Acquisition Regulation 52.232-18, Availability of Funds (Subject to the Availability of Funds) Clause: "SAF" means Subject to Availability of Funds. Funds are not presently available for this contract. The Government's obligation under this contract is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this contract and until the Contractor receives written notice of such availability from the Contracting Officer.

Undelivered Orders (UDO)

An Undelivered Order represents the value of goods and services ordered and obligated that have not been received or for which the government has not completed payment. UDOs include any orders for which an obligation has been made, but delivery or performance has not yet occurred. As such, UDOs are part of the obligated balance of an appropriation. Program Office POCs and COR's are responsible for providing timely and accurate recommendations for UDO de-obligation, partial de-obligation, or continued monitoring, including supporting documentation to substantiate those recommendations.

Contract file content and maintenance:

COR shall maintain a COR file to include a copy of the contract and all modifications, correspondence, invoices/vouchers, financial tracking, reviews, and past performance information. All COR files will be turned in to the CO upon completion of the contract. The COR Contract Checklist shall contain the following:

- A) **Do I have a signed copy of this contract and/or most recent modification for the contract?**
 - Review the terms and conditions of the contract
 - Identify the type of contract (fixed price, time and materials, labor per hour, etc.)
 - Ensure that all modifications are stored with the base contract
- B) **Have the goods and/or services been received?**
 - Perform receiving and acceptance (or rejection) in FFMS within seven days of receipt of goods and/or services

- Identify any goods received and/or services provided, and/or any goods/services invoiced that were NOT in the contract
 - If goods and/or services are rejected, document the rejection:
 - Notify the vendor and Contracting Officer
 - Note the rejection in WebView
- C) **Is there a date stamp on the invoice received?**
- Ensure that the invoice has been date stamped by the Finance Center
- D) **Does the invoice contain all necessary information?**
- Ensure the invoice contains proper information, such as:
 - Invoice number
 - Invoice date
 - Contract number/task order
 - Amount
 - Vendor name
 - Period of performance
 - Determine whether the invoice information matches the contract information
 - If there are any invoice discrepancies, identify the reasons
 - If valid reasons for the discrepancies exist (e.g., “doing business as” name changes), work with the CO to ensure a modification is in place and notate WebView for future reference
- E) **Are the charges in accordance with the contract?**
- Compare invoice details against the summary
 - Reconcile invoice charges against the contract
 - Work with the vendor to review any charges that are unclear
 - Reject the invoice if the charges are not in accordance with the contract:
 - Notify the vendor and Contracting Officer of the rejection
 - Note the rejection in WebView
- F) **Have I reviewed my burn rate report?**
- The COR should maintain a burn rate report for all contracts
 - Review the invoice to ensure it is not a duplicate
 - If it is a duplicate invoice, ensure that there was only one receiving ticket entered into FFMS (financial management system) and reject the invoice
 - many duplicate payments can be prevented by a COR performing a thorough review of the invoice against the contract terms and conditions

Precautionary Measures: The responsibilities and exclusions set forth in this document are

not intended to be all encompassing. As a COR, you are required to consult with the contracting officer when there are questions on your authority. You are NOT authorized to re-delegate your authority. Violation or misuse of your authority could result in abuse of DHS policy and resources at a minimum or monetary loss to the COR or firm involved, disciplinary actions, and other measures, depending on the extent of the offense.

If you have any questions or problems, please contact the Contracting Specialist, (b)(6); (b)(7)(C) at [202-732-(b)(6); (b)(7)(C)]

Appointment Effective and Termination Dates:

Your appointment as the COR under the above numbered contract is effective the date of this letter.

Your appointment as the COR under the above numbered contract is terminated upon receipt of a written notice of termination from the appointing Contracting Officer, the Contracting Officer's successor, or a higher level of authority.

(b)(6); (b)(7)(C)

Signature of Contracting Officer

Effective Date

Acknowledgement Receipt and Acceptance of Appointment:

Please acknowledge receipt and acceptance of this appointment by signing and returning a full copy of this COR Appointment letter to the Contracting Officer or contract administrator/specialist.

I understand and accept my assignment as the COR under 70CTD020P00000016 as outlined in this letter to me dated 9/9/2020.

(b)(6); (b)(7)(C) MPA

Signature of COR

Date

Attachments:

OGE 450, Confidential Financial Disclosure Report (if applicable)

Copy to:

Supervisor

Contractor

Payment Office (as appropriate)

Other Offices (as appropriate)



**U.S. Immigration
and Customs
Enforcement**

9/9/2020

Contracting Officer's Representative (COR) Nomination Letter

Subject: *Nomination of COR*

To: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) **ATD Ops/Intel Western Region**

I hereby nominate (b)(6); (b)(7)(C) *GS-0343-13* for appointment as primary COR for Data Visualization Portal Seats Licenses 70CTD020P00000016. This request is based on the individual's qualifications as described below and the technical and administrative requirements of the anticipated contract, which will require a COR certified at Level II.

a. ***Federal Acquisition Certification for CORs (FAC-COR)*** Level II COR certified as of June 25, 2020. (b)(6); (b)(7)(C) currently has 40 hours of currency for her two year certification anniversary cycle and is currently registered in FAITAS.

b. ***Training qualification*** (b)(6); (b)(7)(C) has completed the following COR trainings:
June 15 – 25, 2020 – FCR 201 Contracting Officers Representative Level II 40 hours
June 30, 2020 – FAC 043 (FED) Ethics & Procurement Integrity for the AWF 1 CLP

c. ***Technical qualifications/experience:*** From October 2013 – June 2016, (b)(6); (b)(7)(C) served as the Program Specialist of the Department of Interior, Bureau of Indian Affairs, Office of Justice Services, District I COR of 10 detention bed contracts, totaling \$2.5 million in annual funding. As the COR, (b)(6); (b)(7)(C) conducted market research, writing Statements of Work, conducted audits of facilities, verified and paid monthly invoices of beds occupied per facility, conducted financial tracking of contract balances, submitted contract modification requests to the Contracting Officer and kept CO apprised of any concerns with the contract facilities.

d. ***COR contact information to include:***

Supervisor: (b)(6); (b)(7)(C) @ice.dhs.gov, (602) 723-(b)(6); (b)(7)(C)
COR: (b)(6); (b)(7)(C) @ice.dhs.gov, (202) 306-(b)(6); (b)(7)(C)
500 12th St, SW, Washington, DC 20536

e. ***Other information as appropriate:*** (b)(6); (b)(7)(C) has been informed of the necessary requirements to maintain her COR II certification.

Based on this nomination, I recognize and acknowledge the primary duties of the COR is to assist the Contracting Officer with monitoring, documentation and evaluating contractor performance of supplies or services delivered within the specified period of performance.

Another very important duty and critical function of the COR is the timely input of contractor performance (when applicable) into the Contractor Performance Assessment Reporting System (CPARS), as specified in Homeland Security Acquisition Manual (HSAM) subchapter 3042.1502. Furthermore, it is understood that DHS leadership considers the duties of a COR vital to the overall success of the Agency in accomplishing its mission. Consistent with this guidance and HSAM 3042.270-1, each appointed COR will include an annual performance appraisal documenting how well the COR functions are performed. The annual performance appraisal will specifically address the five core responsibilities described in HSAM 3042.270-3(b)(1):

- a. *Performing surveillance/inspections/acceptance,*
- b. *Monitoring activities including providing input to contractor performance evaluations,*
- c. *Making recommendations for invoice and payment,*
- d. *Managing Government-furnished property, and*
- e. *Managing contractor employee access to facilities or systems.*

Additionally, as the COR supervisor, I will ensure that the COR has adequate time and resources to perform the COR duties.

(b)(6); (b)(7)(C)

Signature of Supervisor

Date

*Copy to:
COR
Program Officer*



U.S. Immigration
and Customs
Enforcement

9/9/2020

Contracting Officer's Representative (COR) Nomination Letter

Subject: *Nomination of COR*

To: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) **ATD Ops/Intel Western Region**

I hereby nominate (b)(6); (b)(7)(C) GS-0343-13 for appointment as primary COR for Data Visualization Portal Seats Licenses 70CTD020P00000016. This request is based on the individual's qualifications as described below and the technical and administrative requirements of the anticipated contract, which will require a COR certified at Level II.

a. ***Federal Acquisition Certification for CORs (FAC-COR)*** Level II COR certified as of June 25, 2020. (b)(6); (b)(7)(C) currently has 40 hours of currency for her two year certification anniversary cycle and is currently registered in FAITAS.

b. ***Training qualifications:*** (b)(6); (b)(7)(C) has completed the following COR trainings:
June 15 – 25, 2020 – FCR 201 Contracting Officers Representative Level II 40 hours
June 30, 2020 – FAC 043 (FED) Ethics & Procurement Integrity for the AWF 1 CLP

c. ***Technical qualifications/experience:*** From October 2013 – June 2016, (b)(6); (b)(7)(C) served as the Program Specialist of the Department of Interior, Bureau of Indian Affairs, Office of Justice Services, District I COR of 10 detention bed contracts, totaling \$2.5 million in annual funding. As the COR, (b)(6); (b)(7)(C) conducted market research, writing Statements of Work, conducted audits of facilities, verified and paid monthly invoices of beds occupied per facility, conducted financial tracking of contract balances, submitted contract modification requests to the Contracting Officer and kept CO apprised of any concerns with the contract facilities.

d. ***COR contact information to include:***

Supervisor: (b)(6); (b)(7)(C) (b)(6); (b)(7)(C)@ice.dhs.gov, (602) 723- (b)(6); (b)(7)(C)
COR: (b)(6); (b)(7)(C) (b)(6); (b)(7)(C)@ice.dhs.gov, (202) 306- (b)(6); (b)(7)(C)
500 12th St, SW, Washington, DC 20536

e. ***Other information as appropriate.*** (b)(6); (b)(7)(C) has been informed of the necessary requirements to maintain her COR II certification.

Based on this nomination, I recognize and acknowledge the primary duties of the COR is to assist the Contracting Officer with monitoring, documentation and evaluating contractor performance of supplies or services delivered within the specified period of performance.

Another very important duty and critical function of the COR is the timely input of contractor performance (when applicable) into the Contractor Performance Assessment Reporting System (CPARS), as specified in Homeland Security Acquisition Manual (HSAM) subchapter 3042.1502. Furthermore, it is understood that DHS leadership considers the duties of a COR vital to the overall success of the Agency in accomplishing its mission. Consistent with this guidance and HSAM 3042.270-1, each appointed COR will include an annual performance appraisal documenting how well the COR functions are performed. The annual performance appraisal will specifically address the five core responsibilities described in HSAM 3042.270-3(b)(1):

- a. *Performing surveillance/inspections/acceptance,*
- b. *Monitoring activities including providing input to contractor performance evaluations,*
- c. *Making recommendations for invoice and payment,*
- d. *Managing Government-furnished property, and*
- e. *Managing contractor employee access to facilities or systems.*

Additionally, as the COR supervisor, I will ensure that the COR has adequate time and resources to perform the COR duties.

(b)(6); (b)(7)(C)

Name of Supervisor

(b)(6); (b)(7)(C)

Signature of Supervisor

9/9/20

Date

Copy to:
COR
Program Officer



**U.S. Immigration
and Customs
Enforcement**

9/9/2020

Contracting Officer's Representative (COR) Nomination Letter

Subject: *Nomination of COR*

To: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) **ATD Ops/Intel Western Region**

I hereby nominate (b)(6); (b)(7)(C) *GS-0343-13* for appointment as primary COR for Data Visualization Portal Seats Licenses 70CTD020P00000016. This request is based on the individual's qualifications as described below and the technical and administrative requirements of the anticipated contract, which will require a COR certified at Level II.

a. ***Federal Acquisition Certification for CORs (FAC-COR)*** Level II COR certified as of June 25, 2020. (b)(6); (b)(7)(C) currently has 40 hours of currency for her two year certification anniversary cycle and is currently registered in FAITAS.

b. ***Training qualifications:*** (b)(6); (b)(7)(C) has completed the following COR trainings:
June 15 – 25, 2020 – FCR 201 Contracting Officers Representative Level II 40 hours
June 30, 2020 – FAC 043 (FED) Ethics & Procurement Integrity for the AWF 1 CLP

c. ***Technical qualifications/experience:*** From October 2013 – June 2016, (b)(6); (b)(7)(C) served as the Program Specialist of the Department of Interior, Bureau of Indian Affairs, Office of Justice Services, District I COR of 10 detention bed contracts, totaling \$2.5 million in annual funding. As the COR, (b)(6); (b)(7)(C) conducted market research, writing Statements of Work, conducted audits of facilities, verified and paid monthly invoices of beds occupied per facility, conducted financial tracking of contract balances, submitted contract modification requests to the Contracting Officer and kept CO apprised of any concerns with the contract facilities.

d. ***COR contact information to include:***

Supervisor: (b)(6); (b)(7)(C) @ice.dhs.gov, (602) 723-(b)(6); (b)(7)(C)
COR: (b)(6); (b)(7)(C) @ice.dhs.gov, (202) 306-(b)(6); (b)(7)(C)
500 12th St, SW, Washington, DC 20536

e. ***Other information as appropriate:*** (b)(6); (b)(7)(C) has been informed of the necessary requirements to maintain her COR II certification.

Based on this nomination, I recognize and acknowledge the primary duties of the COR is to assist the Contracting Officer with monitoring, documentation and evaluating contractor performance of supplies or services delivered within the specified period of performance.

Another very important duty and critical function of the COR is the timely input of contractor performance (when applicable) into the Contractor Performance Assessment Reporting System (CPARS), as specified in Homeland Security Acquisition Manual (HSAM) subchapter 3042.1502. Furthermore, it is understood that DHS leadership considers the duties of a COR vital to the overall success of the Agency in accomplishing its mission. Consistent with this guidance and HSAM 3042.270-1, each appointed COR will include an annual performance appraisal documenting how well the COR functions are performed. The annual performance appraisal will specifically address the five core responsibilities described in HSAM 3042.270-3(b)(1):

- a. *Performing surveillance/inspections/acceptance,*
- b. *Monitoring activities including providing input to contractor performance evaluations,*
- c. *Making recommendations for invoice and payment,*
- d. *Managing Government-furnished property, and*
- e. *Managing contractor employee access to facilities or systems.*

Additionally, as the COR supervisor, I will ensure that the COR has adequate time and resources to perform the COR duties.

(b)(6); (b)(7)(C)

Signature of Supervisor

Date

*Copy to:
COR
Program Officer*



**U.S. Immigration
and Customs
Enforcement**

9/9/2020

Contracting Officer's Representative (COR) Appointment Letter

Subject: Appointment as a COR

From: (b)(6); (b)(7)(C)

To:

You are hereby appointed as the COR under 70CTD020P00000016 with Venntel, Inc for Data Visualization Portal Seats Licenses. The Contracting Officer will rely on you as a technical expert to provide advice regarding the quality and timeliness of the work performed. As the COR, your primary duties include assisting the Contracting Officer with monitoring the prime contractor's performance; ensuring that all technical requirements under the contract are met; timely delivery of products or services by the delivery date or within the period of performance; and at the price or within the estimated cost stipulated in the contract. The duties or authorities in this letter are not delegable; therefore, you must advise the Contracting Officer, (b)(6); (b)(7)(C) or the Contract Administrator/Specialist (b)(6); (b)(7)(C) immediately when you are unable to perform these duties.

Scope of Authority

COR Responsibilities and Duties

Your duties, as applicable to the contract, are as follows:

I. Performing surveillance/inspection and acceptance, as listed in HSAM-Appendix W, Exhibit 1.

- A) Perform on-site surveillance in accordance with the surveillance plan. Document surveillance activities and provide a copy of documentation to the contracting officer. Review technical proficiency and compliance against the technical provisions of the contract and verify the performance of work by the contractor.
- B) Perform surveillance of the performance under the business agreement and conduct inspections necessary to assure performance and compliance with the terms and conditions of the agreement.

- C) Assure prompt review of draft reports and approval of final reports to contractor to assist with meeting the specified completion date of the contract, and assuring prompt inspection and acceptance, or rejection, of deliverable.
- D) Notify the Contractor of deficiencies observed during surveillance. Record and report to the contracting officer all incidents of faulty or nonconforming work, delays, or problems that may disrupt or hinder future performance.

II. Monitoring activities, cost (see HSAM 3016.601, 3032.7000, and 3042.1500), providing input to contractor performance evaluations and notifications to the Contracting Officer (see examples):

- A) See HSAM 3016.601 and 3032.7000 for specific requirement in monitoring cost reimbursement contracts & time-and-material and labor hour contracts.
- B) For T&M and labor-hour contracts, the COR duties for monitoring contract performance should include, at a minimum, verifying:
 - 1) The work performed is consistent and conforms with the Statement of Work (SOW), Statement of Objectives (SOO), or Performance Work Statement (PWS);
 - 2) The appropriateness of the categories of labor used;
 - 3) The reasonableness of the number of hours worked, including any approved overtime;
 - 4) The reasonableness of materials used; and
 - 5) The hours worked against the hours billed for the invoice period.
 Note, see HSAM Appendix S for a "Payment Approval Template."
- C) For contracts awarded after August 2011 with a dollar value over \$500,000 for supplies and \$1,000,000 for services, enter the contractor performance evaluation information into Contractor Performance Assessment Reporting System (CPARS). Component Head of the Contracting Activity (HCA) are responsible for contractor performance evaluations procedures and policies (see HSAM 3042.1500) for ensuring that contractor performance evaluations (interim and final) are included in the Past Performance Information Retrieval System (PPIRS) through the CPARS. The CO's identification and requested assistance from the COR for input into the contractor evaluations can be efficiently assigned via the appointment COR letter. For access to CPARS, see Section IX, Training.

III. Notification examples:

- 1) Any requests for changes from a contractor.
- 2) Potential labor disputes or workforce problems.
- 3) Lack of performance that may jeopardize the cost or required schedule.
- 4) Monitoring financial management controls with respect to the allocation of appropriated dollars under the designated contract.
- 5) Possible changes in contractor management and/or key personnel.
- 6) Disagreements with the contractor regarding performance of SOW/SOO requirements or other potential disputes with the contractor about technical or other business matters.
- 7) Any possible contractor deficiencies or questionable practices, so that corrections can be made before problems become significant.

- 8) Procurement fraud, waste, abuse, bribery, conflict of interest, or other improper conduct to the CO and agency office, such as the Office of Inspector General (OIG).
- 9) All problems, potential disagreements, or controversy, both oral and in writing, regarding the status of the contract and performance of its requirements.

IV. Making recommendations for invoices and payments (See HSAM 3016.601 and 3032.7000.)

- A) Report any discrepancies in payment vouchers to the CO. Provide documentation to support the representation.
- B) Evaluate progress payment requests based on costs incurred and actual work accomplished.
- C) Certify invoices to the contracting officer for payment, using the electronic invoicing system in FileOnQ – WebView. For Web View training, please visit [OFM website](#).
- D) Reviewing contractor invoices for accuracy of work completed in accordance with contract requirements and certify acceptance or rejection.
- E) Review the contractor's invoices/vouchers for reasonableness and applicability to the contract and recommend to the CO approval, conditional approval, or disapproval for payment. The review must be completed within five days after receipt of the invoice or voucher. If you cannot meet the required review time, advise the CO or contract specialist so that action can be taken to ensure Government compliance with the Prompt Payment Act, thereby avoiding the payment of interest penalties to the contractor.
- F) Review the contractor's invoices/vouchers to ensure that they accurately reflect the work completed in accordance with the requirements of the contract, and certify or reject acceptance of the delivered items. Submit certified invoices/vouchers to the Dallas Finance Center and copies to the CO in a timely manner.
- G) See HSAM 3106.601 and 3032.7000 requirements for processing payment for cost reimbursement and time-and-material and labor hour contracts.

V. Managing Government Furnished Property (used when Government property is specified in the contract).

	YES	NO
Government Furnished Property (GFP)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Government Furnished Equipment (GFE)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- A) You are not authorized to provide any Government-owned (or leased) equipment or supplies or use of Government space to the contractor, other than those specifically identified in the contract and authorized by the Contracting Officer.
- B) If applicable, ensure Government Furnished Property and/or Equipment is made available in a timely manner.
- C) Request the Contracting Officer authorize Government furnished property/equipment, and when requested by the Contracting Officer, provide disposition advice on Government-furnished property/equipment or contractor-acquired property.

VI. Managing Contractor Employee Access and Security through established application process for cards, badges, or credentials (when security requirements are specified in the contract). Exit Checklist MUST be used when contractors leave a contract, move/transfer to a new contract, or is terminated (Click for [Attachment A](#)).

Serves as a Federal sponsor for contractor, by assisting with the agency Security process, to include handling, as appropriate, the Contractor Suitability worksheet for contractor requiring a DHS PIV card, notification of results of the contractor access submissions, ensuring the return of the DHSPIV card, and communication of contractor and employee's changes in status.

VII. Preform oversight of inherently Governmental and critical functions. See HSAM 3007.5 and DHS Guide on Inherently Governmental and Critical Functions regarding specific requirements:

Perform on-going reviews of the functions performed by contractors, especially how work is performed and the manner in which Government personnel are managing services acquisitions. Reviews should focus on functions that are closely associated with inherently governmental functions and critical functions. In addition, monitor contracts to ensure that the relationships between Government personnel and contractors have not evolved into unauthorized personal services or inherently governmental functions. Also, provide information to the CO so the CO can document the contract file to reflect the results of the on-going review.

VIII. Non-Delegable Functions and Exclusions (See HSAM-Appendix W, Exhibit 2 for requirements & HSAM3042.270-3(b)(2)).

As COR you shall not:

- A) Contracting officers may not delegate to the COR the following authorities or activities:
- B) To make or give the appearance of being able to make commitments, modifications, or other actions which would commit the Government to a change in contract price, performance, quality, quantity, or the delivery schedule.
- C) To provide guidance to the contractor, either orally or in writing, which might be interpreted as a change in the scope or terms of the contract.
- D) To change or modify any of the terms and conditions, or statement of work of a contract or business agreement.
- E) To take any action with respect to termination, except to notify the contracting officer that action may be necessary and to assist with the process as requested.
- F) To engage in conduct prejudicial to the Government.
- G) To sign contracts or contract modifications.
- H) To solicit proposals.
- I) To direct a contractor (oral or written) to begin work prior to contract award date or notice to proceed, or to stop work.
- J) To participate in negotiations with a contractor outside of the presence of a contracting officer.
- K) To render a decision on any dispute or question of fact under the Disputes clause of the contract.
- L) To interfere with the contractor's management by supervising contractor employees or otherwise directing their work efforts.

- M) To specify limitations and include the admonition that the COR may be personally liable for unauthorized commitments.
- N) To make any agreement with the contractor relating to the expenditure of Government funds.

IX. FAR and DHS Authorities/Directives, Government Ethics, and Training: (See HSAM 3042.270-3(b)(3)).

Adherence to applicable requirements for ethics (annual training), procurement integrity, no conflict of interest, and proper standards of conduct, including the identification of regulations (e.g., FAR Part 3, Improper Business Practices and Personal Conflicts of Interests), statutes, or agency directives governing these topics (e.g., 5 CFR Part 2635 Standards of Conduct and Management Directive 0480.1, Ethics/Standards of Conduct (or any successor directive)).

Complete and file with the ICE Ethics Office an OGE-450 (Confidential Financial Disclosure Report), via the appropriate confidential report system. Forward your completed OGE-450 as required electronically to the ICE Ethics Office (Office of the Principal Legal Advisor (OPLA)). In addition, you are required to complete annual ethics training as stipulated by the ICE Ethics Official. More information can be found at the [ICE Ethics Intranet Site](#).

Use of authority for appointment letter is “Pursuant to the Federal Acquisition Regulation (FAR), the Homeland Security Acquisition Regulation (HSAR), you are appointed the COR or Alternate COR.”

Training:

Adherence to DHS Annual Skills Currency to maintain COR certification and any other special instructions for obtaining training, to include annual ethics training or other relevant training, as listed in HSAM Appendix W.

In order to obtain access into the CPARS, you are required by ICE/OAQ to take the following courses (CPARS Overview and Quality and Narrative Writing) that are available through the CPARS website (links below). Please contact the ICE Point of Contact, (b)(6); (b)(7)(C) via phone: (202) 732- or email: (b)(7)(E)@ice.dhs.gov or @ice.dhs.gov for questions or assistance.

CPARS Overview (2.25 hours). **Take Training** – This training will give the student an overview of the policies and regulations governing CPARS, the CPARS Workflow, and CPARS Application functionality. Taking the CPARS Overview is a prerequisite to Quality and Narrative Writing and Focal Point Functions.

Quality and Narrative Writing (1.75 hours). **Take Training** – This training will give the student an understanding of the need for quality and accuracy in narrative writing, examples of narratives and resources to aid in creating quality Past Performance Evaluations, and examples of strategies for making the CPARS-FAPIIS process more effective. Taking the CPARS Overview is a prerequisite to taking this class.

Federal Acquisition Certification Requirements.

Based on the technical and administrative characteristics of this contract, I have determined that the COR must possess a Federal Acquisition Certification (FAC) level II. Your appointment as COR is based on the training, experience, certification, and other qualifications cited in your nomination letter. It is your responsibility to maintain your certification and/or qualifications for COR on this contract, including completing continuous learning points. If you fail to maintain your FAC COR certification at this level, DHS is prohibited by law from paying you for performing COR functions.

Please contact the ICE/OAQ Point of Contact: (b)(6); (b)(7)(C) via phone: (202) 732-(b)(6); (b)(7)(C) or email: (b)(6); (b)(7)(C)@ice.dhs.gov for COR/FAC certification/training questions.

As COR you shall be aware of the following:

Federal Acquisition Regulation 52.232-18, Availability of Funds (Subject to the Availability of Funds) Clause: "SAF" means Subject to Availability of Funds. Funds are not presently available for this contract. The Government's obligation under this contract is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this contract and until the Contractor receives written notice of such availability from the Contracting Officer.

Undelivered Orders (UDO)

An Undelivered Order represents the value of goods and services ordered and obligated that have not been received or for which the government has not completed payment. UDOs include any orders for which an obligation has been made, but delivery or performance has not yet occurred. As such, UDOs are part of the obligated balance of an appropriation. Program Office POCs and COR's are responsible for providing timely and accurate recommendations for UDO de-obligation, partial de-obligation, or continued monitoring, including supporting documentation to substantiate those recommendations.

Contract file content and maintenance:

COR shall maintain a COR file to include a copy of the contract and all modifications, correspondence, invoices/vouchers, financial tracking, reviews, and past performance information. All COR files will be turned in to the CO upon completion of the contract. The COR Contract Checklist shall contain the following:

- A) **Do I have a signed copy of this contract and/or most recent modification for the contract?**
 - Review the terms and conditions of the contract
 - Identify the type of contract (fixed price, time and materials, labor per hour, etc.)
 - Ensure that all modifications are stored with the base contract
- B) **Have the goods and/or services been received?**
 - Perform receiving and acceptance (or rejection) in FFMS within seven days of receipt of goods and/or services

- Identify any goods received and/or services provided, and/or any goods/services invoiced that were NOT in the contract
 - If goods and/or services are rejected, document the rejection:
 - Notify the vendor and Contracting Officer
 - Note the rejection in WebView
- C) **Is there a date stamp on the invoice received?**
- Ensure that the invoice has been date stamped by the Finance Center
- D) **Does the invoice contain all necessary information?**
- Ensure the invoice contains proper information, such as:
 - Invoice number
 - Invoice date
 - Contract number/task order
 - Amount
 - Vendor name
 - Period of performance
 - Determine whether the invoice information matches the contract information
 - If there are any invoice discrepancies, identify the reasons
 - If valid reasons for the discrepancies exist (e.g., “doing business as” name changes), work with the CO to ensure a modification is in place and notate WebView for future reference
- E) **Are the charges in accordance with the contract?**
- Compare invoice details against the summary
 - Reconcile invoice charges against the contract
 - Work with the vendor to review any charges that are unclear
 - Reject the invoice if the charges are not in accordance with the contract:
 - Notify the vendor and Contracting Officer of the rejection
 - Note the rejection in WebView
- F) **Have I reviewed my burn rate report?**
- The COR should maintain a burn rate report for all contracts
 - Review the invoice to ensure it is not a duplicate
 - If it is a duplicate invoice, ensure that there was only one receiving ticket entered into FFMS (financial management system) and reject the invoice
 - many duplicate payments can be prevented by a COR performing a thorough review of the invoice against the contract terms and conditions

Precautionary Measures: The responsibilities and exclusions set forth in this document are

not intended to be all encompassing. As a COR, you are required to consult with the contracting officer when there are questions on your authority. You are NOT authorized to re-delegate your authority. Violation or misuse of your authority could result in abuse of DHS policy and resources at a minimum or monetary loss to the COR or firm involved, disciplinary actions, and other measures, depending on the extent of the offense.

(b)(6);
(b)(7)(C)

If you have any questions or problems, please contact the Contracting Specialist, (b)(6); (b)(7)(C) at [202-732-(b)(6); (b)(7)(C)]

Appointment Effective and Termination Dates:

Your appointment as the COR under the above numbered contract is effective the date of this letter.

Your appointment as the COR under the above numbered contract is terminated upon receipt of a written notice of termination from the appointing Contracting Officer, the Contracting Officer's successor, or a higher level of authority.

(b)(6); (b)(7)(C)

Signature of Contracting Officer

Effective Date

Acknowledgement Receipt and Acceptance of Appointment:

Please acknowledge receipt and acceptance of this appointment by signing and returning a full copy of this COR Appointment letter to the Contracting Officer or contract administrator/specialist.

I understand and accept my assignment as the COR under 70CTD020P00000016 as outlined in this letter to me dated 9/9/2020.

(b)(6); (b)(7)(C)

MPA

Signature of COR

Date

Attachments:

OGE 450, Confidential Financial Disclosure Report (if applicable)

Copy to:

Supervisor

Contractor

Payment Office (as appropriate)

Other Offices (as appropriate)

Print Close Help			
Transaction Information			
Award Type:	Purchase Order	Prepared Date:	08/11/2020 22:16:49
Award Status:	Final	Last Modified Date:	09/10/2020 18:32:59
Closed Status:	No	Closed Status Date:	
		Prepared User:	(b)(6); (b)(7)(C) @DHS.GOV
		Last Modified User:	(b)(6); (b)(7)(C) @DHS.GOV
		Closed By:	
Document Information			
Award ID:	(b)(7)(E)	Procurement Identifier	70CTD020P00000016
Referenced IDV ID:		Modification No	0
Reason For Modification:			
Solicitation ID:			
	Agency Identifier	Main Account	Sub Account
Treasury Account Symbol:			
		Initiative	Select One
Dates		Amounts	
Date Signed:	09/10/2020	Action Obligation:	\$40,000.00
Period of Performance Start Date:	09/11/2020	Base And Exercised Options Value:	\$40,000.00
Completion Date:	09/10/2025	Base and All Options Value (Total Contract Value):	\$200,000.00
Est. Ultimate Completion Date:	09/10/2025	Fee Paid for Use of Indefinite Delivery Vehicle:	\$0.00
Solicitation Date:	07/23/2020		
Purchaser Information			
Contracting Office Agency ID:	7012	Contracting Office Agency Name:	U.S. IMMIGRATION AND CUSTOMS ENF
Contracting Office ID:	(b)(7)(E)	Contracting Office Name:	INFORMATION TECHNOLOGY DIVISION
Funding Agency ID:	7012	Funding Agency Name:	U.S. IMMIGRATION AND CUSTOMS ENF
Funding Office ID:	(b)(7)(E)	Funding Office Name:	ENFORCMNT&REMOVL OPNS HQ ENF M
Foreign Funding:	Not Applicable		
Contractor Information			
SAM Exception:	... Remove Exception		
DUNS No:	080601076	Street:	2201 COOPERATIVE WAY STE 600
Vendor Name:	VENNTEL, INC.	Street2:	
DBAN:		City:	HERNDON
Cage Code:	7UV15	State:	VA
		Zip:	201713005
		Country:	UNITED STATES
		Phone:	(571) 758 (b)(6); (b)(7)(C)
		Fax No:	
		Congressional District:	VIRGINIA 11
Business Category		Show Details	
Organization Type	CORPORATE NOT TA	Business Types	
State of Incorporation	DE	<input checked="" type="checkbox"/> Corporate Entity, Not Tax Exempt Relationship With Federal Government <input checked="" type="checkbox"/> All Awards Organization Factors <input checked="" type="checkbox"/> For Profit Organization	
Country of Incorporation	USA		
Contract Data			
Type of Contract:	Firm Fixed Price		
Inherently Governmental Functions:	Select One		
Multiyear Contract:	Select One		
Major Program:			
National Interest Action:	None		
Cost Or Pricing Data:	Select One		
Purchase Card Used As Payment Method:	No		
Undefinited Action:	No		
Performance Based Service Acquisition:	Not Applicable		
* FY 2004 and prior; 80% or more specified as performance requirement * FY 2005 and later; 50% or more specified as performance requirement			
Emergency Acquisition:	Not Applicable		
Contract Financing:			

Cost Accounting Standards Clause:		Select One
Consolidated Contract:		Select One
Number Of Actions:		Not Consolidated
		1
Legislative Mandates		Principal Place of Performance
Clinger-Cohen Act:	No	Principal Place Of Performance State Location Country
Labor Standards:	Not Applicable	Code: DC USA
Materials, Supplies, Articles, and Equip:	Not Applicable	Principal Place Of Performance DISTRICT OF COLUMBIA
Construction Wage Rate Requirements:	Not Applicable	County Name:
	Select One or More Options	Principal Place Of Performance WASHINGTON
	Employment Eligibility Verification (52.222-54)	City Name:
	Service Contract Inventory (FAR 4.17)	Congressional District Place Of Performance: 00
Additional Reporting:		Place Of Performance Zip Code (+4): 20536 - 0001
Interagency Contracting Authority:	Not Applicable	
Other Interagency Contracting Statutory Authority: (1000 characters)		
<div></div>		
Product Or Service Information		
Product/Service Code:	7030	Description: INFORMATION TECHNOLOGY SOFTWARE
Principal NAICS Code:	541519	Description: OTHER COMPUTER RELATED SERVICES
Bundled Contract:	Not Bundled	
DOD Acquisition Program:		
Country of Product or Service Origin:	USA UNITED STATES	
Place of Manufacture:	Mfg in U.S.	
Domestic or Foreign Entity:	U.S. Owned Business	
Recovered Materials/Sustainability:	No Clauses Included and No Sustainability Included	OMB Policy on Sustainable Acquisition
InfoTech Commercial Item Category:	Select One	
Claimant Program Code:		Description:
Sea Transportation:	Select One	
GFP Provided Under This Action:	Transaction does not use GFP	
Use Of EPA Designated Products:	Not Required	
Description Of Requirement: (Limit 250 characters)	DATA VISULIZATION PORTAL SOFTWARE	
Current: 33		
Competition Information		
Extent Competed For Referenced IDV:		
Extent Competed:	Not Competed under SAP	
Source Selection Process:	Other	
Solicitation Procedures:	Simplified Acquisition	
IDV Type Of Set Aside:		
Type Of Set Aside:	No set aside used.	
Type Of Set Aside Source:	This Action	
Evaluated Preference:	No Preference used	
SBIR/STTR:	Select One	
Fair Opportunity/Limited Sources:	Select One	
Other Than Full And Open Competition:	SAP Non-Competition (FAR 13)	
Local Area Set Aside:	No	
FedBizOpps:	Not Applicable	
A76 Action:	No	
Commercial Item Acquisition Procedures:	Commercial Item	
IDV Number of Offers:		
Number Of Offers Received:	1	Number of Offers Source: This Action
Small Business Competitiveness Demonstration Program:		
Simplified Procedures for Certain Commercial Items:	No	
Preference Programs / Other Data		

Contracting Officer's Business Size Selection:

Small Business

Subcontract Plan:

Plan Not Required

Price Evaluation Percent Difference:

%

HSAM Appendix G - Checklist for Sensitive Information

Procurement Title: Data Visualization Portal Seats

Requisition #: 192120ATDOPI20002

Estimated Contract Value (incl. options): \$200,000

Instructions: The requiring office shall complete this checklist for all acquisitions, including assisted acquisitions, regardless of dollar value. A properly executed checklist serves as the high risk determination required by HSAR Class Deviation 15-01, Safeguarding of Sensitive Information. If the requiring official determines that a contractor will have access to sensitive information and/or contractor IT systems will be used to input, store, process, output and/or transmit sensitive information, the requiring official shall ensure the Statement of Work, Statement of Objective, Performance Work Statement or specification is reviewed by the organizations identified at HSAM 3004.470(b) and obtain signatures, as applicable, on this checklist. If it is not clear to the requiring official if the contractor will have access to sensitive information and/or if contractor IT systems will be used to input, store, process, output, and/or transmit sensitive information, the requirements official shall at a minimum consult with the Component Chief Information Officer (CIO), Chief Security Officer (CSO) and Privacy Officer. The requiring office shall submit the completed checklist as part of the procurement request package in accordance with HSAM 3004.7101. Failure to submit a completed checklist will result in the return of the procurement request package. The contracting officer is responsible for routing the checklist to the Head of Contracting Activity (HCA) or designee for signature and ensuring the solicitation and resultant contract reflect the requirements contained in the checklist.

A. Sensitive Information and Access Requirements (completed by the requiring office):

1. Will the contractor have access to any of the types of the sensitive information listed below during the acquisition?

<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	<div style="border: 1px solid black; padding: 2px;">(b)(7)(E)</div>
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	For Official Use Only (FOUO)
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	Law Enforcement Sensitive Information
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	Protected Critical Infrastructure Information (PCII)
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	Personally Identifiable Information (PII)
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	Sensitive PII (SPII)
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	Sensitive Security Information (SSI)
<input type="checkbox"/> Other type of sensitive information		

2. Will contractor employees have access to DHS information systems? ☐ Yes ☒ No

3. Will contractor employees require recurring access to Government facilities?

☐ Yes ☒ No

Note: If the answer is “No” to questions 1 through 3, proceed to the Signatures section of the checklist. When the answer is “No” to questions 1 through 3, the checklist shall, at a minimum, be signed by the requiring official and the HCA (or designee).

4. If the answer is “Yes” to either of questions 1 through 3 above, confirm that information security, personnel security, and/or privacy provisions have been identified for inclusion in the solicitation and resultant contract and coordinated with the following, as applicable (see HSAM 3004.470(b) for coordination requirements).

Definitions:

- **Information security provisions** include the development of the Requirements Traceability Matrix, identification of incident reporting and response requirements, and requests for the contractor to: provide security authorization documentation, obtain an independent assessment, perform continuous monitoring, provide the Government with necessary access to perform security reviews, comply with federal reporting requirements.
- **Personnel security provisions** include reviewing fitness requirements and other security matters related to access to sensitive but unclassified information and recurring access of contractor employees to Government facilities, information systems, security items or products.
- **Privacy provisions** include requirements for handling PII and/or SPII, incident reporting, notification and credit monitoring.

- | | | | |
|------------------------------|-----------------------------|---|--|
| <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input checked="" type="checkbox"/> N/A | Component CIO or designee |
| <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input checked="" type="checkbox"/> N/A | Component CSO or designee |
| <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input checked="" type="checkbox"/> N/A | Component Privacy Officer |
| <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input checked="" type="checkbox"/> N/A | TSA SSI Program Office |
| <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input checked="" type="checkbox"/> N/A | Cybersecurity and Infrastructure Security Agency (CISA) CVI Program Office |
| <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input checked="" type="checkbox"/> N/A | CISA PCII Program Office |

Note: For Components and offices that do not have a Component level CIO, CSO, or Privacy Officer, the requiring official shall coordinate with the DHS Headquarters CIO, CSO and Chief Privacy Officer (or designee for each). (See HSAM 3004.470(b)(7))

5. Has the Component CIO, CSO, Privacy Officer, HCA (or designee for each) and program manager determined that this effort will have a “high risk” of unauthorized access to or disclosure of sensitive information in accordance with the requirements of HSAR Deviation 15-01, Safeguarding of Sensitive Information, applicable to this acquisition?
☐ Yes ☒ No

Note: If the answer to this question is “Yes” special clauses Safeguarding of Sensitive Information (MAR 2015), Information Technology Security and Privacy Training (MAR

2015) and HSAR clause 3052.204-71 Contractor Employee Access shall be included without revision in the solicitation and subsequent contract (as defined in FAR 2.101).

6. If the answer is “Yes” to any of the preceding questions, identify and describe the information security, personnel security, and privacy provisions to be included in the solicitation including the special clauses from HSAR Class Deviation 15-01, Safeguarding of Sensitive Information if applicable.

N/A

7. If foreign end products or services are allowed under the contract, what additional security provisions are to be included in the solicitation to protect sensitive information and facilities from unauthorized access and disclosure?

N/A

B. Authority to Operate (ATO) and Continuous Monitoring Data Requirements (completed by requiring office in coordination with Component CIO or designee):

1. Will contractor IT systems be used to input, store, process, output, and/or transmit sensitive information? ☐ Yes ☒ No
2. If “Yes” to #1, has the requiring office coordinated development of the Requirements Traceability Matrix (RTM) with the Component CIO or designee for inclusion in the solicitation? ☐ Yes ☒ N/A (only if “No” to #1)
3. If “Yes” to #1, will the solicitation require the submission of a draft security plan and instructions on how the draft security plan will be evaluated? ☐ Yes ☒ N/A (only if “No” to #1)

4. If “Yes” to #1, does the requirements document identify how the contractor should submit monthly continuous monitoring data to the Government? ☐ Yes ☒ N/A (only if “No” to #1)
5. If “Yes” to #1, identify and describe the continuous monitoring data requirements to be included in the solicitation.

N/A

Note: When a contractor IT system will be used to input, store, process, output, and/or transmit sensitive information, the RTM shall be included in the solicitation. The RTM is prepared by the Component CIO or designee in coordination with the requiring office and shall be included in the procurement request package as an attachment to the requirements document (i.e., Statement of Work, Statement of Objectives, Performance Work Statement). Contracting officers shall ensure the solicitation requires vendors to submit a draft security plan with their proposal/quotation as their response to the RTM. Instructions on how the draft security plan will be evaluated shall be included in the solicitation.

C. Data Retention Requirements (completed by requiring office):

1. Will the contractor be required to retain sensitive information for the Government?
☐ Yes ☒ No
2. If “Yes” to #1, does the requirements document identify (a) retention requirements (e.g., length of time data must be retained before return and/or destruction) and (b) security requirements for the protection of retained data? ☐ Yes ☒ N/A (only if “No” to #1)
3. If “Yes” to #1, identify and describe the retention and security requirements to be included in the solicitation.

N/A

4. Does the Government have a plan to monitor and/or ensure contractor compliance with the retention and security requirements identified? ☐ Yes ☒ N/A (only if “No” to #1)
5. If “Yes” to #1, describe the Government’s plan to monitor and/or ensure contractor compliance with the retention and security requirements identified in the acquisition.

N/A

D. Additional Privacy Considerations (completed by requiring office in coordination with Component Privacy Officer or designee):

1. Is contractor support needed to complete privacy compliance documentation (Privacy Threshold Analysis, Privacy Impact Assessment, and/or System of Record Notice, as appropriate)? ☐ Yes ☐ No ☒ N/A
2. If contractor support is needed to complete the privacy compliance documentation, does the requirements document identify the activities and level of contractor support needed? ☐ Yes ☒ N/A (only if “No” or “N/A” to #1)
3. If “Yes” to #1, identify and describe the activities and level of contractor support needed to complete the privacy compliance documentation.

N/A

Signatures:

	Signature	DHS Component and Organization	Telephone Number
Requiring Official (or official title)	(b)(6); (b)(7)(C)	ICE/ERO/Custody Management/ Alternatives to Detention (ATD)	D: 202-732- (b)(6); (b)(7)(C) C: 202-271-
Component Chief Information Officer (CIO) or designee		ICE/OCIO/Information Assurance Division (IAD)	(b)(6); (b)(7)(C)
Component Chief Security Officer (CSO) or designee		ICE/OPR/Office of Professional Responsibility (OPR)	
Component Privacy Officer or designee		ICE/Office of Information Government & Privacy (IGP)	
TSA SSI Program Office, as applicable			
CISA CVI Program Office, as applicable			
CISA PCII Program Office, as applicable			
Head of Contracting Activity (HCA) or designee		ICE/Office of Acquisition Management (OAQ)	(b)(6); (b)(7)(C)

If the answer is “No” to the first three questions within this form, the Contracting Officer is to sign as the HCA

(b)(6); (b)(7)(C)

Name:

Contracting Officer / Head of Contracting Activity Designee

Office of Acquisition Management (OAQ)

Phone:

Attachment B

Program Office Code ICE-ERO-CUSTODY MANAGEMENT-ALTERNATIVES TO DETENTION					
Requisition Number : 192120ATDOI20002 Title: Data Visualization Portal Subscription					
Independent Government Cost Estimate					
Cost Category	Description	Unit of Measurement	Quantity	Rate	Total
Service	Data Visualization Portal Subscription Service - Base Year	ea	(b)(4); (b)(7)(E)		
Service	Data Visualization Portal Subscription Service - Option Year 1	ea			
Service	Data Visualization Portal Subscription Service - Option Year 2	ea			
Service	Data Visualization Portal Subscription Service - Option Year 3	ea			
Service	Data Visualization Portal Subscription Service - Option Year 4	ea			
				Estimated Firm Fixed Price	\$ 200,000.00
Estimated Contract Total:					\$ 200,000.00

Attachment B

Program Office Code ICE-ERO-CUSTODY MANAGEMENT-ALTERNATIVES TO DETENTION					
Requisition Number : 192120ATDOPI20002 Title: Data Visualization Portal Subscription					
Independent Government Cost Estimate					
Cost Category	Description	Unit of Measurement	Quantity	Rate	Total
Service	Data Visualization Portal Subscription Service	ea	(b)(4); (b)(7)(E)		
Estimated Firm Fixed Price				\$	40,000.00
Estimated Contract Total:				\$	40,000.00

**Program Office Code ICE-ERO-Custody Management-Alternatives to Detention
Requisition Number 192120ATDOPI20002 Data Visualization Subscription Portal**

Independent Government Cost Estimate

Cost Category	Description	Unit of Measuremen	Quantity	Rate	Total
Service	Data Visualization (Geolocation) Portal Service Subscription	ea	(b)(4); (b)(7)(E)		
Estimated Total Firm Fixed Price					\$ 40,000.00
Estimated Contract Total:					\$ 40,000.00
		\$	-		

Program Office Code ICE-ERO-Custody Management-Alternatives to Detention Requisition Number 192120ATDOPI20002 Data Visualization Subscription Portal					
Independent Government Cost Estimate					
Cost Category	Description	Unit of Measurement	Quantity	Rate	Total
Service	Data Visualization (Geolocation) Portal Service Subscription	ea	(b)(4); (b)(7)(E)		
Estimated Total Firm Fixed Price				\$	40,000.00
Estimated Contract Total:				\$	40,000.00
		\$	-		

Program Office Code ICE-ERO-Custody Management-Alternatives to Detention Requisition Number 192120ATDOPI20002 Data Visualization Subscription Portal					
Independent Government Cost Estimate					
Cost Category	Description	Unit of Measurement	Quantity	Rate	Total
Service	Data Visualization (Geolocation) Portal Service Subscription	ea	(b)(4); (b)(7)(E)		
Estimated Total Firm Fixed Price					\$ 40,000.00
Estimated Contract Total:					\$ 40,000.00
		\$	-		

Program Office Code ICE-ERO-Custody Management-Alternatives to Detention Requisition Number 192120ATDOPI20002 Data Visualization Subscription Portal					
Independent Government Cost Estimate					
Cost Category	Description	Unit of Measurement	Quantity	Rate	Total
Service	Data Visualization (Geolocation) Portal Service Subscription	ea	(b)(4); (b)(7)(E)		
Estimated Total Firm Fixed Price					\$ 40,000.00
Estimated Contract Total:					\$ 40,000.00
		\$	-		

Justification for Other Than Full and Open Competition

Pursuant to the requirements of 41 U.S.C. 3304 as implemented by FAR Subpart 6.3, and IAW the requirements of FAR Subpart 6.303-1, the justification for the use of the statutory authority under FAR Subpart 6.3 is justified by the following facts and rationale required under FAR Subpart 6.303-2 as follows:

1. Agency and Contracting Activity

Department of Homeland Security
Immigration and Customs Enforcement
Office Acquisition Management, Information Technology Division
801 I Street, NW
Washington, DC 20536

2. Nature and/or Description of the Action Being Approved

DHS ICE is proposing to enter into a sole source contract between Venntel Inc. and ERO. The proposed contract will be for one (1) year, with four (4) option years, during which time Venntel Inc. will provide ERO with access to their proprietary software portal and data subscription service and access to the Venntel Data Science Team to request custom data pulls, unique data insights, and analysis support.

3. Description of Supplies/Services

Venntel Inc. will allow ERO to access/gain information to support the Government's requirement to accurately identify digital devices within the borders of the United States, and internationally, sharing their information at a specific location, or a designated polygon area, during a specified time period during the preceding 90 and up to 180 days. Venntel Inc. will allow access to the Venntel global mobile location database via their web portal to identified users capable of sending 12,000 queries annually aggregated across total user population.

The base period of performance is September 11, 2020 through September 10, 2021, with four (4) one-year option periods. The costs of the solution are listed below.

Period	Quantity	Unit Price	Total Price
Base Year	12 months	(b)(4)	
Option Year 1	12 months		
Option Year 2	12 months		
Option Year 3	12 months		
Option Year 4	12 months		
		Totals	\$200,000

4. Identification of Statutory Authority Permitting Other Than Full and Open Competition

The statutory authority permitting other than full and open competition is 41 U.S.C. 253(c)(1) implemented by Federal Acquisition Regulation (FAR) Subpart 6.302-1 entitled “Only One Responsible Source and No Other Supplies or Services Will Satisfy Agency Requirements.”

5. Demonstration that the Contractor’s Unique Qualifications or the Nature of the Acquisition Requires the Use of the Authority Cited

The Venntel platform is user friendly and simple to operate, as it clearly identifies the information requirements needed to initiate the search parameters. The search results can be viewed directly in the platform or downloaded to an Excel file and manipulated by law enforcement personnel for analysis. The ability of law enforcement to successfully and efficiently review the data; of multiple or single devices greatly increases the chances of ERO officers apprehending an absconder.

(b)(7)(E)

6. Efforts to Obtain Competition

Efforts were made to promote competition by searching for companies that offered similar software. The other vendor used social media to compile information, which is not easily accessible within the ICE network. ERO’s Alternatives to Detention (ATD) program, participated in a pilot project with the personnel from the Combined Intelligence Unit (CIU); the project’s objective was to locate and apprehend ATD Absconders. Locate X and Venntel were two companies that were contacted to verify whether they could meet ERO’s needs.

Services provided by both platforms allow law enforcement personnel to draw a geo-fence around an address or general location, which identifies the latitude and longitude coordinates of multiple mobile devices that were located within the selected area for the timeframe searched. The identified devices can then be searched independently and with a new search timeframe, to obtain a history of locations and/or coordinates the device was recorded at. The searching of the device’s location history allows for law enforcement personnel to establish patterns of life and identify potential residences or places of employment of absconders.

The results of this exercise showed that only one vendor met all of the requirements and demonstrated an interest in working with ICE:

Venntel, Inc.
Attn: (b)(6); (b)(7)(C)
2201 Cooperative Way
Suite 600
Herndon, VA 20171
703-989-(b)(6);
(b)(7)(C)

7. Determination by the Contracting Officer that the Anticipated Cost to the Government Will be Fair and Reasonable

ICE determined the proposed price by Venntel, Inc. for the Data Visual Portal Seats software was fair and reasonable based historical information/market research of a comparison of the prices submitted. Venntel, Inc. also included pricing for the four one-year option periods.

8. Description of Market Research

Efforts were made to promote competition by searching the internet for data visual software that meet all the ICE ERO's requirements.

9. Any Other Facts Supporting the Use of Other than Full and Open Competition

N/A

ICE has found no alternatives available to provide secure all-inclusive solution with a very competitive pricing, support, and training to end user.

10. A Listing of the Sources, if any, that Expressed in Writing an Interest in the Acquisition

N/A

11. A Statement of the Actions, if any, the Agency May Take to Remove or Overcome any Barriers to Competition Before any Subsequent Acquisition for Supplies or Services Required

N/A

12. Certifications

Note: The certification page should be the last page of the J&A on a separate page. Obtain all necessary concurrences and approvals.

I certify that the facts and representations under my cognizance, which are included in this justification, meet the Government's minimum need and that the supporting data, which forms a basis for this justification, is complete and accurate.

Requirements/Technical Personnel:

(b)(6); (b)(7)(C)

9/9/2020

Date

Technical Representative

Contracting Officer:

I certify that the justification is accurate and complete to the best of my knowledge and belief.

(b)(6); (b)(7)(C)

9/10/2020

Date

Contracting Officer

From: (b)(6); (b)(7)(C)
Sent: 11 Sep 2020 21:03:16 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: 70CTD020P00000016

My pleasure.

Thank you, you too!

Respectfully,

(b)(6); (b)(7)(C) **MSCJ/MBA/MSM**
Information Technology Division (ITD) | Contract Specialist
DHS | ICE | Office of Acquisition Management (OAQ)
801 I Street, N.W.
Washington, DC 20536-5750
Phone: 202-732- Fax: 202-732-7369
E-mail: (b)(6); (b)(7)(C)@ice.dhs.gov

From: (b)(6); (b)(7)(C)@venntel.com>
Sent: Friday, September 11, 2020 4:49 PM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>
Cc: (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)@ice.dhs.gov>
Subject: Re: 70CTD020P00000016

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact [ICE SOC SPAM](#) with questions or concerns.

Thank you (b)(6); (b)(7)(C) I will get this processed on our end. Have a great weekend.

Sent from my iPhone

On Sep 11, 2020, at 4:43 PM, (b)(6); (b)(7)(C)@ice.dhs.gov> wrote:

Good Afternoon:

Attached is the Fiscal Year 2020 Purchase Order between U.S. Immigration and Customs Enforcement (ICE) and Venntel, Inc. for Data Visualization Portal Seats.

Please feel free to contact me should you have any questions or concerns regarding the this e-mail.

Thank you.

Respectfully,

(b)(6); (b)(7)(C) **MSCJ/MBA/MSM**
Information Technology Division (ITD) | Contract Specialist
DHS | ICE | Office of Acquisition Management (OAQ)
801 I Street, N.W.
Washington, DC 20536-5750
Phone: 202-732-(b)(6); (b)(7)(C) Fax: 202-732-7369
E-mail: (b)(6); (b)(7)(C)@ice.dhs.gov
<70CTD020P00000016.pdf>
<Statement of Work.pdf>

This message is private and confidential and is intended only for the recipient specified in this message. If you received this message in error, please notify the sender by reply transmission and deleting the message. If you are not the intended recipient, any use, disclosure, dissemination, distribution, publication, or copying of this message and its contents is strictly prohibited.

From: (b)(6); (b)(7)(C)
Sent: 23 Jul 2020 14:34:30 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: Venntel Quote (ICE ERO ATD)_March 19 2020.pdf

Good Morning (b)(6); (b)(7)(C)

Thank you for your quotation. I have forwarded the quotation to the end user to confirm that it meets her technical needs.

Respectfully,

(b)(6); (b)(7)(C) **MSCJ/MBA/MSM**
Information Technology Division (ITD) | Contract Specialist
DHS | ICE | Office of Acquisition Management (OAQ)
801 I Street, N.W.
Washington, DC 20536-5750
Phone: 202-732-(b)(6); (b)(7)(C) Fax: 202-732-7369
E-mail: (b)(6); (b)(7)(C)@ice.dhs.gov

From: (b)(6); (b)(7)(C)@venntel.com>
Sent: Thursday, July 23, 2020 10:30 AM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>
Cc: (b)(6); (b)(7)(C)@venntel.com>; (b)(6); (b)(7)(C)@venntel.com>
Subject: Re: Venntel Quote (ICE ERO ATD)_March 19 2020.pdf

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact ICE SOC SPAM with questions or concerns.

Good Morning (b)(6); (b)(7)(C)

Thanks for your inquiry to Venntel. (b)(6); (b)(7)(C) is no longer with the company and I will be managing his responsibilities.

Attached you will find the updated quote with the 4 option years as you requested. Let me know if you have any questions. I am happy to setup a quick call to go over the details.

Kind regards.

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)@venntel.com>
Date: July 22, 2020 at 4:18:17 PM EDT
To: (b)(6); (b)(7)(C)@venntel.com>; (b)(6); (b)(7)(C)@venntel.com>
Subject: Venntel Quote (ICE ERO ATD)_March 19 2020.pdf
Reply-To: (b)(6); (b)(7)(C)@ice.dhs.gov>

Good Afternoon (b)(6); (b)(7)(C)

My name is (b)(6); (b)(7)(C) and I am a Contract Specialist with the U.S. Immigration and Customs Enforcement. I received a quote for Data Visualization Portal Seats. I was hoping that you could provide me with an updated quote, inclusive of 4 optional years.

Please feel free to contact me should you have any questions or concerns regarding this e-mail.

Thank you.

Respectfully,

(b)(6); (b)(7)(C) **MSCJ/MBA/MSM**
Information Technology Division (ITD) | Contract Specialist
DHS | ICE | Office of Acquisition Management (OAQ)
801 I Street, N.W.
Washington, DC 20536-5750
Phone: 202-732-(b)(6); (b)(7)(C) Fax: 202-732-7369
E-mail: (b)(6); (b)(7)(C)@ice.dhs.gov

(b)(6);
(b)(7)(C)

--

(b)(6); (b)(7)(C)

Director of Government Sales, Venntel

(703) 989- (b)(6); (b)(7)(C) @venntel.com

venntel.com

Request a Demo

This message is private and confidential and is intended only for the recipient specified in this message. If you received this message in error, please notify the sender by reply transmission and deleting the message. If you are not the intended recipient, any use, disclosure, dissemination, distribution, publication, or copying of this message and its contents is strictly prohibited.

(b)(6);
(b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 22 Jul 2020 20:18:14 +0000
To: (b)(6); (b)(7)(C)@venntel.com
Subject: Venntel Quote (ICE ERO ATD)_March 19 2020.pdf
Attachments: Venntel Quote (ICE ERO ATD)_March 19 2020.pdf

Good Afternoon (b)(6); (b)(7)(C)

My name is (b)(6); (b)(7)(C) and I am a Contract Specialist with the U.S. Immigration and Customs Enforcement. I received a quote for Data Visualization Portal Seats. I was hoping that you could provide me with an updated quote, inclusive of 4 optional years.

Please feel free to contact me should you have any questions or concerns regarding this e-mail.

Thank you.

Respectfully,

(b)(6); (b)(7)(C) **MSCJ/MBA/MSM**
Information Technology Division (ITD) | Contract Specialist
DHS | ICE | Office of Acquisition Management (OAQ)
801 I Street, N.W.
Washington, DC 20536-5750
Phone: 202-732- (b)(6); (b)(7)(C) Fax: 202-732-7369
E-mail: (b)(6); (b)(7)(C)@ice.dhs.gov

(b)(6);
(b)(7)(C)

From: ICATT.Alert
Sent: 15 Sep 2020 20:04:32 +0000
To: #ICEOCRTaskings
Subject: -20-03735- CNGR Inquiry - Contract Award to Venntel ICATT:0045244

Hello OCR,

A Clearance has been assigned to you. Please accept in 1 day

Clearance Name: CL-20-03735 Assigned To OCR

Due Date: 09/24/2020 12:00 PM Eastern

Instructions:

Please supply response to document using track changes.

Thank you,

ICATT System

From: (b)(6); (b)(7)(C)
Sent: 28 Aug 2020 14:36:51 +0000
To: (b)(6); (b)(7)(C)
Subject: FW: URGENT--CNGR Inquiry - Contract Award to Venntel

FYSA [redacted] and colleagues-

No action needed.

Synopsis:

The DHS' Chief Procurement Officer reached out directly to component Heads of Contract Activity (HCAs) for information responsive to a congressional inquiry. I have asked for the original congressional inquiry to get details on the full "ask".

EAD Barrera asked her team to loop us in for proper coordination, which is when I was tagged. I'm working with ESEC and ICE OAQ on it now and will keep you apprised.

(b)(5)

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Date: Friday, Aug 28, 2020, 10:15 AM
To: (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: RE: URGENT--CNGR Inquiry - Contract Award to Venntel

Hi (b)(6); (b)(7)(C)

(b)(5); (b)(6); (b)(7)(C)

Thank you!

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) @ice.dhs.gov>
Date: Friday, Aug 28, 2020, 9:59 AM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: RE: URGENT--CNGR Inquiry - Contract Award to Venntel

Hi (b)(6);
(b)(7)(C)

(b)(6); (b)(7)(C) DHS Chief Procurement Officer, tasked all of the DHS Heads of Contracting Activity to provide the data this week.

OAQ answered a Congressional Inquiry before in June for Sen. Markey. OAQ Dallas awarded one additional order to Venntel since that Congressional Inquiry Response was provided. Before we awarded the June purchase order, (b)(6); (b)(7)(C) coordinated with (b)(6); (b)(7)(C) Privacy and

(b)(6); (b)(7)(C) (b)(5)
(b)(5)

Let me know if you want to have a call about this to discuss more details.

V/r

(b)(6); (b)(7)(C)
Chief of Staff
Office of Acquisition Management (OAQ)
U.S. Immigration and Customs Enforcement
Desk Phone: 202-732 (b)(6);
(b)(7)(C)
Cell Phone: 202-906- (b)(6);
(b)(7)(C)
Email: (b)(6); (b)(7)(C) @ice.dhs.gov

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Sent: Friday, August 28, 2020 9:41 AM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: RE: URGENT--CNGR Inquiry - Contract Award to Venntel

(b)(6); (b)(7)(C); (b)(5)

Thanks!

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Date: Friday, Aug 28, 2020, 9:38 AM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: RE: URGENT--CNGR Inquiry - Contract Award to Venntel

(b)(6); (b)(7)(C) can you let (b)(6); (b)(7)(C) know if there is an incoming letter?

(b)(5)

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Sent: Friday, August 28, 2020 9:27 AM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: RE: URGENT--CNGR Inquiry - Contract Award to Venntel

Thank you (b)(6); (b)(7)(C) agree. Is there an incoming letter from the Member/Committee/Staffer?

We will look for the formal tasking through ICATT and will coordinate.

Thank you!

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Date: Friday, Aug 28, 2020, 9:17 AM
To: Bailey, Jason (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: FW: URGENT--CNGR Inquiry - Contract Award to Venntel

(b)(6); (b)(7)(C)

Please see below e-mail chain. (b)(5)

(b)(5)

Can you coordinate with (b)(6); (b)(7)(C) appropriate?

Thanks,

(b)(6); (b)(7)(C)

From: (b)(7)(E)@sp.ice.dhs.gov

Sent: 3 Jan 2018 14:47:19 -0500

To: (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Subject: New task from HQEXOPS: 92009 - RFI - S1 Immigration and Border Security Part II - January 11th - Law Enforcement FOLDERID 92009

Attachments: S-S2 Briefing Memo-Meeting Template.docx

Please do not reply to this e-mail. It is from an unmonitored system account. All action should occur within OESIMS.

Due Date:

1/3/2018 5:00:00 PM

Instructions:

ICE EXECUTIVE SECRETARY TASKINGS

Request for Information

*S1 Immigration and Border Security Part II - January 11th - Law Enforcement
92009*

Program-Level Clearance Required: SES

Tasking Assignments:

Program Assignment	Program	Due Date	Time
Lead Program	HSI Taskings	1/3/2018	NLT 5PM
Non-Lead Program	ERO Taskings	1/3/2018	NLT 5PM
Non-Lead Program	OCR Taskings	1/4/2018	NLT 11AM
Review	OPLA Taskings	1/4/2018	NLT 1PM

- OES is not responsible for coordinating or consolidating Program Office responses.
- The lead program office must reconcile all ICE intra-agency comments and/or questions prior to closing their task bar.

Instructions:

- **Please provide information on the attached Briefing Memo template on Law Enforcement and specifically on:**
 - **Sanctuary Cities**
 - **Gang Activities**
 - **TCOs**
 - **Cell Site Simulators**

- Please provide your response in the required format, template, font, and page amount stated.
- Pay close attention to the proper use of acronyms and that ICE is the overall stated agency response.
- Any Law Enforcement Sensitive information provided must be labeled correctly.
- Program offices are required to review and edit all responses prior to submission.
- Immediately contact ICE Taskings if you believe a program with equities has been inadvertently overlooked.

Failure to complete any of the above requirements will result in a re-task.

Background:

This information will be used by S1 for upcoming hearing on immigration and border security.

Thank you,

(b)(6); (b)(7)(C)

Taskings Assistant
Executive Secretary Tasking
Office of the Director
U.S. Immigration and Customs Enforcement
202.732 (b)(6);
(b)(7)(C)
(b)(7)(E)@ice.dhs.gov

This message is part of an automated workflow, please do not change the text in the subject line when responding or forwarding the message.

Folder Subject: 92009 - RFI - S1 Immigration and Border Security Part II - January 11th
- Law Enforcement

Folder Originator: DHS

Due Date: 1/3/2018 5:00:00 PM

Workflow ID: (b)(7)(E)

Folder Location:

(b)(7)(E)

Task ID: (b)(7)(E)

Workflow Task ID: (b)(7)(E)

Assignment ID: (b)(7)(E)

FOR OFFICIAL USE ONLY

(b)(5)

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

(b)(5)



FOR OFFICIAL USE ONLY

From: (b)(7)(E)@sp.ice.dhs.gov

Sent: 24 Jan 2018 16:55:58 -0500

To: (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Subject: New task from HQEXOPS: 92307 - RFI - Query about FOUO/LES status of Dec 4 DHS letter to Sen Wyden FOLDERID 92307

Attachments: ICE Response Template.docx

Please do not reply to this e-mail. It is from an unmonitored system account. All action should occur within OESIMS.

Due Date:

1/25/2018 10:00:00 AM

Instructions:

ICE EXECUTIVE SECRETARY TASKINGS

Request for Information

Query about FOUO/LES status of Dec 4 DHS letter to Sen Wyden

92307

Program-Level Clearance Required: STANDARD

Tasking Assignments:

-

Assignment	Tasking	Due Date	Owner
Program	ings	018	AM
rogram	kings	018	AM
rogram	sking	018	AM
w	ings	018	PM
w	kings	018	PM

-

- OES is not responsible for coordinating or consolidating Program Office responses.
- The lead program office must reconcile all ICE intra-agency comments and/or questions prior to closing their task bar.

Instructions:

-

(b)(5)

(b)(5)

- Please provide your response in the required format, template, font, and page amount stated.
- Pay close attention to the proper use of acronyms and that ICE is the overall stated agency response.
- Any Law Enforcement Sensitive information provided must be labeled correctly.
- Program offices are required to review and edit all responses prior to submission.
- Immediately contact ICE Taskings if you believe a program with equities has been inadvertently overlooked.

Failure to complete any of the above requirements will result in a re-task.

Thank you,

(b)(6); (b)(7)(C)

Taskings Assistant
Executive Secretary Tasking
Office of the Director
U.S. Immigration and Customs Enforcement
(202) 732-
Unclass: (b)(7)(E)@ice.dhs.gov

Original Message:

This message is part of an automated workflow, please do not change the text in the subject line when responding or forwarding the message.

Folder Subject: 92307 - RFI - Query about FOUO/LES status of Dec 4 DHS letter to Sen Wyden

Folder Originator: DHS

Due Date: 1/25/2018 10:00:00 AM

Workflow ID: (b)(7)(E)

Folder Location:

(b)(7)(E)

Task ID: (b)(7)(E)

Workflow Task ID: (b)(7)(E)

Assignment ID: (b)(7)(E)



U.S. Immigration and Customs Enforcement
Response to Query about FOUO/LES status of Dec 4 DHS letter to Sen Wyden
Month 1, 2017

(b)(5)

FOR OFFICIAL USE ONLY // LAW ENFORCEMENT
SENSITIVE

1

From: (b)(7)(E)@sp.ice.dhs.gov

Sent: 19 Jan 2018 16:49:11 -0500

To: (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Subject: New task from HQEXOPS: 92307 - RFI - Query about FOUO/LES status of Dec 4 DHS letter to Sen Wyden FOLDERID 92307

Attachments: SA7PY01200017120414420_0003.pdf, 1149112- Franken +3 082417 Incoming.pdf, ICE Response Template.docx

Please do not reply to this e-mail. It is from an unmonitored system account. All action should occur within OESIMS.

Due Date:

1/22/2018 11:00:00 AM

Instructions:

ICE EXECUTIVE SECRETARY TASKINGS

Review & Comment

*Query about FOUO/LES status of Dec 4 DHS letter to Sen Wyden
92307*

Program-Level Clearance Required: STANDARD

Tasking Assignments:

Program Assignment	Program	Due Date	Time
Lead Program	OPR Taskings	1/22/2018	NLT 11AM
Non-Lead Program	IGP Taskings	1/22/2018	NLT 12:30PM
Non-Lead Program	HSI Taskings	1/22/2018	NLT 12:30PM
Non-Lead Program	ERO Taskings	1/22/2018	NLT 12:30PM
Non-Lead Program	Policy Tasking	1/22/2018	NLT 12:30PM
Review	OCR Taskings	1/22/2018	NLT 1:30PM
Review	OPLA Taskings	1/22/2018	NLT 2:30PM

- OES is not responsible for coordinating or consolidating Program Office responses.
- The lead program office must reconcile all ICE intra-agency comments and/or questions prior to closing their task bar.

Instructions:

- **Please review the response to Question 5a in the ICE Response Template and advise whether it rises to the level of FOUO/LES. If so, provide justification for maintaining the marking, together with a revised response that would bring it below the FOUO/LES threshold.**
- Pay close attention to the proper use of acronyms and that ICE is the overall stated agency response.
- Any Law Enforcement Sensitive information provided must be labeled correctly.
- Program offices are required to review and edit all responses prior to submission.
- Immediately contact ICE Taskings if you believe a program with equities has been inadvertently overlooked.

Failure to complete any of the above requirements will result in a re-task.

Thank you,

(b)(6); (b)(7)(C)

Taskings Assistant
Executive Secretary Tasking
Office of the Director
U.S. Immigration and Customs Enforcement
(202) 732-
Unclass: (b)(7)(E)@ice.dhs.gov
Original Message:

This message is part of an automated workflow, please do not change the text in the subject line when responding or forwarding the message.

Folder Subject: 92307 - RFI - Query about FOUO/LES status of Dec 4 DHS letter to Sen Wyden

Folder Originator: DHS

Due Date: 1/22/2018 11:00:00 AM

Workflow ID: (b)(7)(E)

Folder Location:

(b)(7)(E)

Task ID: (b)(7)(E)

Workflow Task ID: (b)(7)(E)

Assignment ID: (b)(7)(E)



Homeland
Security

December 4, 2017

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

Thank you for your August 24, 2017 letter. Acting Secretary Duke asked that I respond on her behalf.

For specific responses to each of your questions, please refer to the enclosure. To address your specific concern related to U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO) utilizing cell-site simulators, I can confirm that ICE/ERO does not use cell-site simulators for the purpose of civil immigration law enforcement. While ICE/ERO's primary mission is to enforce the Nation's civil immigration laws, individual ERO officers may participate in Joint Task Forces with federal, state, and local law enforcement partners, in furtherance of our shared public safety mission. Such Joint Task Forces may employ various technologies, including cell-site simulator technology, to pursue individuals suspected of engaging in criminal activity. However, such use must be conducted in a manner that protects rights afforded by the U.S. Constitution, and in compliance with applicable statutory authorities.

While cell-site simulators are used by several Components of the Department of Homeland Security (DHS), no Component is using this technology for the purpose of civil immigration enforcement. ICE Homeland Security Investigations (HSI) uses cell-site simulators in support of criminal investigations requiring judicial process, and not for administrative violations under the Immigration and Nationality Act. ICE/HSI's use of cell-site simulator technology in the context of criminal investigations, may result in the arrest of aliens unlawfully present in the United States who are the targets of said criminal investigations.

U.S. Customs and Border Protection (CBP) has made limited use of cell-site simulators. CBP's Office of Professional Responsibility has used this technology in support of ongoing criminal investigations related to employee integrity and workforce security.

(b)(7)(E)

The Honorable Ron Wyden
Page 2

The DHS Components that use cell-site simulators do so in a manner that is consistent with DHS Policy Directive 047-02, *Department Policy Regarding the Use of Cell-Site Simulator Technology*, dated October 19, 2015, which closely aligns with the Department of Justice's policy guidance regarding the use of cell-site simulator technology. Under current policy, absent exigent circumstances under the Fourth Amendment or other exceptional circumstances where the law does not require a search warrant, operators must obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or applicable state equivalent).

The technology is typically used to either locate a subject using their mobile device, or to determine which mobile device (i.e., smartphone) a subject is carrying. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

When used to identify a mobile device carried by a suspect, it provides investigators with information that can then be used to subpoena the phone records for that device. (b)(7)(E)

(b)(7)(E)

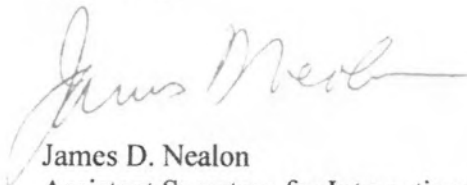
When practicable and based on the totality of circumstances, investigators will attempt to locate the target of an investigation using traditional investigative techniques prior to deploying a cell-site simulator. Additionally, investigators will only deploy the cell-site simulator in the general geographic area of the targeted mobile handset for the minimum amount of time needed to determine the location of the target of the criminal investigation.

When cell-site simulators are in use, interference with non-targeted mobile devices is virtually non-existent. The mobile identifier of non-targeted mobile handsets is automatically verified by the cell-site simulators as a non-target and sent back to the host mobile network. This process is conducted in an amount of time that is not noticeable to the user. If a call is placed or received during the exact instant the verification is taking place, interference may result. Cell-site simulators used by DHS include software that has provisions to allow a captured device (i.e., one currently engaged by the cell-site simulator) to return to the host network if the captured device initiates a call. Devices are always able to dial 911 without any disruption of service. DHS remains committed to ensuring law enforcement practices concerning the collection or retention of data are lawful and respect the important privacy interests of individuals.

The Honorable Ron Wyden
Page 3

Thank you again for your letter and interest in this important matter. The cosigners of your letter will receive separate, identical responses. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

A handwritten signature in cursive script, appearing to read "James D. Nealon", written in dark ink.

James D. Nealon
Assistant Secretary for International Affairs
Office of Strategy, Policy, and Plans

Enclosure

**The Department of Homeland Security's Response to
Senator Al Franken's August 24, 2017 Letter**

1. **Policy Directive 047-02 “applies to the use of CSS technology inside the United States in furtherance of criminal investigations.” According to ICE, CSS devices are used “in support of criminal investigations requiring judicial process, and not for administrative violations under the Immigration and Nationality Act.” ICE has also stated that ICE Enforcement and Removal Operations (ERO) “does not use cell-site simulators for the purpose of civil immigration enforcement.”**
 - a. **In the Department's use of CSS technology for criminal investigations, does DHS distinguish between the seriousness of criminal offenses in determining whether to deploy CSS technology? If so, how?**

Neither the Department of Homeland Security (DHS) nor its Components have specifically prioritized criminal offenses for this purpose.

U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) does not have a protocol designating a specific list of priority violations. In the event of limited resources, ICE HSI prioritizes cell-site simulator (CSS) deployments based on mission needs.

(b)(7)(E)

U.S. Customs and Border Protection's (CBP) Office of Professional Responsibility has made very limited use of CSS technology, and only in support of criminal investigations related to employee integrity and workforce security.

- b. **The Department's response to Senator Wyden's May 23, 2017 letter confirmed that ERO does not use CSS devices for administrative immigration enforcement. Does any other Component within the Department use CSS technology pursuant to non-criminal investigations within the United States.**

Within DHS, ICE HSI and USSS are the predominant users of CSS devices, and CBP has made limited use of this technology. No DHS Component uses CSS technology for the purpose of civil immigration enforcement or other “non-criminal” investigations.

2. Policy Directive 047-02 states that “[a]ffected DHS Components may issue additional specific guidance consistent with this policy.” Please provide copies of all such additional specific guidance, if any, issued by DHS’s immigration enforcement Components.

ICE HSI has issued internal guidance that is consistent with the October 19, 2015 DHS Policy Directive 047-02, *Department Policy Regarding the Use of Cell-Site Simulator Technology*, as well as the Department of Justice’s *Guidance on the Use of Cell-Site Simulator Technology*. CBP is in the process of developing internal operational policy governing the use of CSS technology.

3. Policy Directive 047-02 provides that DHS Components shall implement an auditing program to ensure that data collected by CSS technology is deleted following the completion of a mission, upon location of a target, and upon the identification of a target. Are such audits performed by Components that use CSS technology for immigration enforcement? If not, why?
- a. If so, how frequently are such audits performed?
 - b. If so, what have such audits revealed about DHS Components’ data collection, retention, and disposal practices?

DHS Components do not use CSS technology for administrative immigration violations.

4. Policy Directive 047-02 provides that “DHS is committed to ensuring that law enforcement practices concerning the collection and retention of data are lawful and respect the important privacy interests of individuals.” Furthermore, in response to Senator Wyden’s letter, ICE stated that ICE Homeland Security Investigations operates CSS devices “in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information.”
- a. Aside from Policy Directive 047-02, what “rules, policies, and laws” apply to information collected through the use of CSS technology? In particular, what “rules, policies, and laws” apply to information about noncitizens obtained through the use of CSS technology?

DHS uses CSS devices in a manner consistent with the requirements and protections of the Constitution, including the Fourth Amendment and applicable statutory authorities, including the Pen Register Statute (18 U.S.C. §§ 3121 *et seq.*). DHS Components’ CSS use is also guided by DHS Policy Directive 047-02 and Component policy.

Pursuant to Department Policy, absent exigent circumstances under the Fourth Amendment or other exceptional circumstances where the law does not require a search warrant, operators are required to obtain a search warrant supported by probable cause

and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or applicable state equivalent). Nationality and/or citizenship are not considered when deploying these devices; DHS Components deploy the devices only with probable cause supporting that an individual is suspected of committing a criminal violation.

Information that ICE HSI collects from CSS devices that is relevant to an investigation is recorded in Reports of Investigations, which are stored in the appropriate investigative file and retained in accordance with the applicable federal records schedule. Information that is not relevant to an investigation is not retained. Any information that ICE collects from CSS devices pertaining to U.S. citizens or Lawful Permanent Residents (LPRs) is used and disclosed in accordance with the DHS ICE – 009 External Investigations System of Records Notice.¹ Finally, any information ICE obtains from CSS devices pertaining to individuals who are neither U.S. citizens nor LPRs is handled in accordance with the Fair Information Practice Principles as outlined in DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*.² In addition to those protections, any information ICE obtains from these devices pertaining to individuals that may have applied or been granted U Nonimmigrant Status, T Nonimmigrant status, or protections under the *Violence Against Women Act* are handled in accordance with 8 U.S.C. Section 1367.

- b. **Section 14 of President Trump’s Executive Order, entitled *Enhancing Public Safety in the Interior of the United States*, seeks to remove Privacy Act protections from immigrants who are not U.S. citizens or permanent residents. What effect does Section 14 of the President’s January 25, 2017 Executive Order have on the Department’s data collection and disposal policies, including but not limited to those laid out in Policy Directive 047-20?**

Section 14 of President Trump’s Executive Order, *Enhancing Public Safety in the Interior of the United States*, will not change how DHS and, specifically, ICE collects or disposes of data obtained through CSS devices.

5. **Policy Directive 047-02 provides that an application or supporting affidavit should inform the court that the target cell phone and other cell phones in the area of the CSS device might experience a temporary disruption of service from the service provider. In response to Senator Wyden’s letter, ICE stated that “[d]uring use of cell-site simulators, interference with non-targeted mobile devices is virtually non-existent.” ICE also stated that “[i]n all circumstances, devices are always able to dial 911 without any disruption of service.” Please describe, in detail, how DHS knows this to be the case “in all circumstances.”**

¹ See DHS/ICE – External Investigations System of Records Notice, (75 FR 404, Jan. 5, 2010), available at:

(b)(7)(E)

- a. Have DHS employees (rather than manufacturers or third parties) tested the CSS technology the Department uses to measure the interference caused to nearby phones? If so, please provide a copy of all testing reports or other documentation related to device and network interference caused by CSS technology.

Neither ICE nor USSS has funded independent interference testing. Components rely on manufacturer specifications and their extensive experience with the technology in the field.

With respect to your question about disruption of service, when CSS devices are in use, the mobile identifier of non-targeted mobile handsets is automatically verified by the device as a non-target and sent back to the host mobile network. This process is conducted in an amount of time that is not noticeable to the user. If a call is placed or received during the exact instant the verification is taking place, interference may result. CSSs used by DHS include software that has provisions to allow a captured device (i.e., one currently engaged by the CSS) to return to the host network if the captured device initiates a call. In all circumstances, devices are always able to dial 911 without any disruption of service.

DHS is not aware of any complaints or reports of network interference or disruption from the CSS technology used by DHS.

6. Does DHS maintain a record of which components possess CSS technology; how many CSS devices each component has; the makes and models of CSS devices used by each component; and when, where, and for how long the devices are used for immigration enforcement? If so, please provide a copy of such records.

(b)(7)(E) DHS does not maintain a centralized repository of this information. Currently, ICE HSI has ☐ CSSs in operation, USSS has ☐ and CBP has ☐ ³ CSSs are used in support of criminal investigations, requiring judicial process, and are not utilized for administrative violations under the Immigration and Nationality Act. The makes and models of CSS equipment utilized by DHS are considered law enforcement sensitive. DHS personnel may be made available to discuss equipment specifics should a briefing be deemed necessary. (b)(7)(E)

7. Does DHS maintain a record of how many individuals have been located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology? If so, please provide a copy of such records and state how many of the individuals located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology have been arrested for a crime, convicted of a crime, and convicted of a violent crime.

DHS does not use CSS for administrative immigration violations.

³ CBP's recent use has been in coordination with ICE/HSI, using an ICE-owned device, operated by ICE personnel. November 2017

8. Does DHS deploy CSS technology for immigration enforcement purposes along the nation's borders? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.

No.

9. Does DHS deploy CSS technology during interior immigration enforcement? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.

No.

United States Senate
WASHINGTON, DC 20510

SCANNED/RECEIVED
BY ESEC SEC

2017 AUG 24 PM 3:22

August 24, 2017

The Honorable Elaine C. Duke
Acting Secretary of Homeland Security
U.S. Department of Homeland Security
Washington, DC 20528

Dear Acting Secretary Duke:

In light of reports that federal authorities deployed cell-site simulator (CSS) technology during an immigration raid, we write to request additional information about the Department of Homeland Security's (DHS) use of these powerful surveillance devices in immigration enforcement actions.¹ While we appreciate the need for federal law enforcement agencies to locate and track dangerous suspects, we are concerned that using CSS technology during immigration enforcement actions poses a significant risk to privacy and civil liberties.

CSS devices—commonly known as “stingrays” or International Mobile Subscriber Identity Catcher devices (IMSI-catchers)—are portable surveillance devices that mimic cellphone towers and compel affected mobile phones to reveal their location and registration information. In recognition of the important privacy concerns raised by the use of CSS technology, in October 2015 DHS issued a policy directive on the Department's use of such devices (Policy Directive 047-02).² The directive “applies to the use of CSS technology inside the United States in furtherance of criminal investigations,” and it requires DHS's law enforcement components to obtain a search warrant supported by probable cause before deploying CSS technology. The directive also imposes some appropriate limits on cell phone data collection and retention. However, because the directive's scope only applies to criminal investigations, it does not apply to the administrative investigations that make up a substantial portion of DHS's immigration enforcement actions.

A recently published federal search warrant affidavit revealed publicly for the first time that an Immigration and Customs Enforcement (ICE) officer used a CSS device to track the location of an undocumented immigrant.³ In that particular case, according to the affidavit, DHS was conducting a criminal investigation of the undocumented immigrant for violation of 8 U.S.C. §1326(a).⁴ Accordingly, a federal judge issued a warrant authorizing, among other things, the use of a CSS device.

¹ Alvaro M. Bedoya, *Deportation Is Going High-Tech Under Trump*, THE ATLANTIC, June 21, 2017, at <https://www.theatlantic.com/technology/archive/2017/06/data-driven-deportation/531090/>.

² U.S. Department of Homeland Security, Policy Directive 047-02, Department Policy Regarding the Use of Cell-Site Simulator Technology (Oct. 19, 2015), at <https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf>.

³ Robert Snell, *Feds use anti-terror tool to hunt the undocumented*, DETROIT NEWS, May 18, 2017, at <http://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616/>.

⁴ Search Warrant Affidavit for *The Cellular Device Assigned Call Number (XXX) XXX-XXXX*, Eastern District of Michigan, no. 2:17-mc-50368-01 (2017), at <https://www.documentcloud.org/documents/3727182-CSS1.html>.

In response to questions raised by Senator Wyden,⁵ ICE clarified that it deploys CSS devices only in support of “criminal investigations requiring judicial process,” and that it “does not use cell-site simulators for the purpose of civil immigration enforcement.”⁶ ICE also explained that it continues to apply the limitations set forth in Policy Directive 047-02 to its use of CSS technology. However, significant questions remain about the Department’s use of CSS technology for immigration enforcement purposes, such as the extent of the technology’s deployment in our cities and neighborhoods, and what additional safeguards are in place to protect the privacy and civil liberties of our immigrant communities. In an effort to gain a better understanding of how DHS’s immigration enforcement officers are using CSS technology, we respectfully request that you provide individual responses to each of the following questions:

1. Policy Directive 047-02 “applies to the use of CSS technology inside the United States in furtherance of criminal investigations.” According to ICE, CSS devices are used “in support of criminal investigations requiring judicial process, and not for administrative violations under the Immigration and Nationality Act.” ICE has also stated that ICE Enforcement and Removal Operations (ERO) “does not use cell-site simulators for the purpose of civil immigration enforcement.”
 - a. In the Department’s use of CSS technology for criminal investigations, does DHS distinguish between the seriousness of criminal offenses in determining whether to deploy CSS technology? If so, how?
 - b. The Department’s response to Senator Wyden’s May 23, 2017 letter confirmed that ERO does not use CSS devices for administrative immigration enforcement. Does any other component within the Department use CSS technology pursuant to non-criminal investigations within the United States?
2. Policy Directive 047-02 states that “[a]ffected DHS Components may issue additional specific guidance consistent with this policy.” Please provide copies of all such additional specific guidance, if any, issued by DHS’s immigration enforcement components.
3. Policy Directive 047-02 provides that DHS components shall implement an auditing program to ensure that data collected by CSS technology is deleted following the completion of a mission, upon location of a target, and upon the identification of a target. Are such audits performed by components that use CSS technology for immigration enforcement? If not, why?
 - a. If so, how frequently are such audits performed?
 - b. If so, what have such audits revealed about DHS components’ data collection, retention, and disposal practices?

⁵ Letter from Ron Wyden, U.S. Senator, to Thomas D. Homan, Acting Director of U.S. Immigration & Customs Enforcement (May 23, 2017), at <https://www.wyden.senate.gov/download/?id=F268CF50-4BF1-41A4-860A-8CED078CAB4A&download=1>.

⁶ Letter from Thomas D. Homan, Acting Director of U.S. Immigration & Customs Enforcement, to Ron Wyden, U.S. Senator (Aug. 16, 2017), at <https://assets.documentcloud.org/documents/3935329/88437-Signed-Response.pdf>.

4. Policy Directive 047-02 provides that "DHS is committed to ensuring that law enforcement practices concerning the collection and retention of data are lawful and respect the important privacy interests of individuals." Furthermore, in response to Senator Wyden's letter, ICE stated that ICE Homeland Security Investigations operates CSS devices "in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personally identifiable information."
 - a. Aside from Policy Directive 047-02, what "rules, policies, and laws" apply to information collected through the use of CSS technology? In particular, what "rules, policies, and laws" apply to information about noncitizens obtained through the use of CSS technology?
 - b. Section 14 of President Trump's Executive Order, entitled *Enhancing Public Safety in the Interior of the United States*, seeks to remove Privacy Act protections from immigrants who are not U.S. citizens or permanent residents. What effect does Section 14 of the president's January 25, 2017 executive order have on the Department's data collection and disposal policies, including but not limited to those laid out in Policy Directive 047-02?
5. Policy Directive 047-02 provides that an application or supporting affidavit should inform the court that the target cell phone and other cell phones in the area of the CSS device might experience a temporary disruption of service from the service provider. In response to Senator Wyden's letter, ICE stated that "[d]uring use of cell-site simulators, interference with non-targeted mobile devices is virtually non-existent." ICE also stated that "[i]n all circumstances, devices are always able to dial 911 without any disruption of service." Please describe, in detail, how DHS knows this to be the case "in all circumstances."
 - a. Have DHS employees (rather than manufacturers or third parties) tested the CSS technology the Department uses to measure the interference caused to nearby phones? If so, please provide a copy of all testing reports or other documentation related to device and network interference caused by CSS technology.
6. Does DHS maintain a record of which components possess CSS technology; how many CSS devices each component has; the makes and models of CSS devices used by each component; and when, where, and for how long the devices are used for immigration enforcement? If so, please provide a copy of such records.
7. Does DHS maintain a record of how many individuals have been located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology? If so, please provide a copy of such records and state how many of the individuals located, tracked, and/or monitored by federal immigration enforcement officers using CSS technology have been arrested for a crime, convicted of a crime, and convicted of a violent crime.

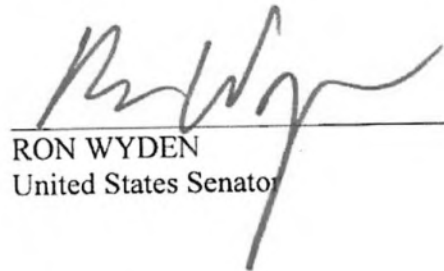
8. Does DHS deploy CSS technology for immigration enforcement purposes along the nation's borders? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.
9. Does DHS deploy CSS technology during interior immigration enforcement? If so, please provide a list of the cities and states in which DHS has deployed CSS technology for immigration enforcement purposes.

Thank you for your prompt attention to this important matter.

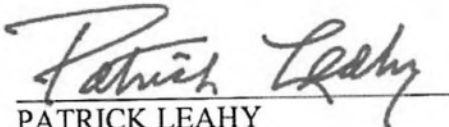
Sincerely,



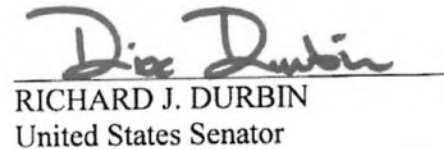
AL FRANKEN
United States Senator



RON WYDEN
United States Senator



PATRICK LEAHY
United States Senator



RICHARD J. DURBIN
United States Senator



U.S. Immigration and Customs Enforcement
Response to Title
Month 1, 2017

(b)(5)

~~FOR OFFICIAL USE ONLY // LAW ENFORCEMENT~~
~~SENSITIVE~~

RE: ICE Emails

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Date: Friday, Sep 18, 2020, 10:31 AM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>,
(b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: RE: ICE Emails

(b)(6);
(b)(7)(C)

(b)(6); (b)(7)(C); (b)(5)

(b)(6);
(b)(7)(C)

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Sent: Thursday, September 17, 2020 5:29 PM
To: (b)(6); (b)(7)(C) @ice.dhs.gov> (b)(6); (b)(7)(C) @ice.dhs.gov>;
(b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov> (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: RE: ICE Emails

All,

Thanks for the heads up. Can my office please receive a copy of the formal ask?

Thanks,

(b)(6);
(b)(7)(C)

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Sent: Thursday, September 17, 2020 5:25 PM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>, (b)(6); (b)(7)(C) @ice.dhs.gov>

(b)(6); (b)(7)(C) @ice.dhs.gov>

Subject: FW: ICE Emails

(b)(6); (b)(7)(C)

Wanted to make you aware of the ask from the House Oversight Committee.

(b)(6); (b)(7)(C)

(A)DAD

Domestic Operations

D 202-732 (b)(6); (b)(7)(C)

C 619-730 (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) @ice.dhs.gov>

Sent: Thursday, September 17, 2020 3:58 PM

To: (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>

Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) @ice.dhs.gov>

Subject: RE: ICE Emails

Fellows adding (b)(6); (b)(7)(C) from OCR.

Sent with BlackBerry Work

(www.blackberry.com)

From: (b)(6); (b)(7)(C) @ice.dhs.gov>

Date: Thursday, Sep 17, 2020, 3:56 PM

To: (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>

Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>

Subject: FW: ICE Emails

FYSA BELOW.

Sent with BlackBerry Work

(www.blackberry.com)

From: (b)(6); (b)(7)(C) @ice.dhs.gov>

Date: Thursday, Sep 17, 2020, 3:54 PM

To: (b)(6); (b)(7)(C) @ice.dhs.gov>

Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>

Subject: FW: ICE Emails

(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) of significance. Pls see below.

(b)(6);
(b)(7)(C)

have you notified HQ?

Regards,

(b)(6); (b)(7)(C)

Deputy Special Agent in Charge
HSI DC

From: (b)(6); (b)(7)(C)@ice.dhs.gov>

Date: Thursday, Sep 17, 2020, 12:16 PM

To: (b)(6); (b)(7)(C)@ice.dhs.gov>

Cc: (b)(6); (b)(7)(C)@ice.dhs.gov> (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)@ice.dhs.gov>

Subject: FW: ICE Emails

(b)(6);
(b)(7)(C)

I received the email below from Venntel indicating they received a request from the House Oversight Committee to deliver to them any emails between ICE and Venntel.

(b)(5)

(b)(6);
(b)(7)(C)

(b)(6);
(b)(7)(C)

(b)(6);
(b)(7)(C)



(b)(6); (b)(7)(C)

Homeland Security Investigations (HSI)
Chief Intelligence Officer
Washington D.C. | Virginia | West Virginia
O: (703) 285- (b)(6);
C: (215) 558- (b)(7)(C)
Email: (b)(6); (b)(7)(C)@ice.dhs.gov
SIPR/HSDN: (b)(6); (b)(7)(C)@dhs.sgov.gov
JWICS/CLAN: (b)(6); (b)(7)(C)@dhs.ic.gov

~~Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this report should be furnished to the media, either in written or verbal form.~~

From: (b)(6); (b)(7)(C)@venntel.com>

Sent: Wednesday, September 16, 2020 12:24 PM

To: (b)(6); (b)(7)(C)@ice.dhs.gov>

Subject: ICE Emails

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact ICE SOC SPAM with questions or concerns.

(b)(6); (b)(7)(C)

Venntel received a request from the House Oversight Committee to deliver to them any emails between ICE and Venntel.

We would like to provide ICE with all of the emails so that your agency has the opportunity to review and redact as needed.

I've tried a number of other contacts that redirected me to privacy lawyers but that ended in a dead-end.

Can you provide me with a good contact I can work with?

Feel free to call me at 571.420. (b)(6); (b)(7)(C)

Thanks

(b)(6);
(b)(7)(C)

571.758 (b)(6); (b)(7)(C) @venntel.com
www.venntel.com

This message is private and confidential and is intended only for the recipient specified in this message. If you received this message in error, please notify the sender by reply transmission and deleting the message. If you are not the intended recipient, any use, disclosure, dissemination, distribution, publication, or copying of this message and its contents is strictly prohibited.

From: (b)(6); (b)(7)(C)
Sent: 4 Nov 2020 19:59:58 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: Venntel Congressional files

Hello (b)(6); (b)(7)(C)

Thank you for the quick response. Correct, the documents located within SharePoint site are the documents that Venntel collected and shared with HSI/Intel to review for redaction. I will reach out to (b)(6); (b)(7)(C)

Thank you.

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)@ice.dhs.gov>
Date: Wednesday, Nov 04, 2020, 11:05 AM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>
Cc: (b)(6); (b)(7)(C)@ice.dhs.gov>
Subject: RE: Venntel Congressional files

Good morning, (b)(6); (b)(7)(C)

Thank you for reaching out. The incoming congressional letter was addressed to the President of Venntel, not ICE. Therefore, OCR would not be involved in transmitting their response back to Congress. I am assuming the documents in the sharepoint folder are documents Venntel collected and shared with HIS/Intel to review for any redactions before transmitting to Congress. You should definitely reach out to (b)(6); (b)(7)(C) Chief OPLA GILD for guidance on ICE's obligation with respect to the letter.

v/r,

(b)(6); (b)(7)(C)

Department of Homeland Security
U.S. Immigration and Customs Enforcement
Office of Congressional Relations

202-732 (b)(6); (b)(7)(C) (direct)
202-732 (b)(6); (b)(7)(C) (main)
202-732-4269 (fax)

From: (b)(6); (b)(7)(C)@ice.dhs.gov>
Sent: Wednesday, November 4, 2020 10:08 AM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>
Cc: (b)(6); (b)(7)(C)@ice.dhs.gov>

Subject: Venntel Congressional files

Importance: High

Good morning (b)(6);
(b)(7)(C)

I am the Section Chief for the Technology Innovation and Management Section (TIPMS) within HSI/Intel. My section reviewed files pertaining to the Venntel Congressional inquiry into the collection and sale of sensitive mobile phone location data. Please see attached document for reference.

I understand that OCR is responsible for providing the response to Congress and I am trying to determine how we should proceed with the redaction process and what else will be needed from HSI/Intel. Will OPLA be involved? Please let me know at your earliest convenience. The summary of the finding are listed below:

Summary

(b)(5)

Additional information regarding the Outlook emails, PowerPoint (PPT) presentations, Excel files and Geolocation files retrieved from Venntel:

- The data/emails were categorized as follows:
 - Personally Identifiable - 8 emails containing 104 documents were categorized as Personally Identifiable
 - Technical Emails - **39** emails containing **20** documents were categorized as Investigative emails
 - Tradecraft Methods and Techniques - **107** emails containing **82** documents were categorized as Tradecraft Methods and Techniques
 - Investigative emails - **90** emails containing **106** documents were categorized as Technical emails. This group includes emails requesting geolocation with only VENNTEL ID's (no PII or other identifying information).
- The majority of the emails and data contained PII, Investigative info and search/tradecraft methods on how to use Venntel. There were many overlaps in categorizing the data. For example, emails containing Investigative Tradecraft Methods overlapped on most occasions. Best judgement was used to determine which category the data most appropriately fit. Batch emails from a single email thread were grouped together and placed into one category.

The communications were between Venntel and HSI offices (mostly Intel offices/ Field and HQ).

The data is stored on SharePoint and is located here:

(b)(7)(E)

Thank you.

(b)(6); (b)(7)(C)

Section Chief
Enterprise Services Division
Technology, Innovation, and Project Management Section
U.S. Immigration and Customs Enforcement
Homeland Security Investigations/Intelligence

Unclass (b)(6); (b)(7)(C) @ice.dhs.gov

HSDN: (b)(6); (b)(7)(C) dhs.sgov.gov

Office (202) 732- (b)(6);
Cell (202) 465- (b)(7)(C)

"If everyone is thinking alike, then somebody isn't thinking."

From: ICATT.Alert
Sent: 28 May 2019 13:30:42 +0000
To: #ICEOCRTaskings
Subject: Review and Comment -P-107334- R&C - FY 2019 DHS Appropriations
Requirement: Cell-Site Simulator Congressional Report ICATT:0045740

Hello OCR,

A Clearance has been assigned to you. Please accept in 1 day

Clearance Name: CL-Tsk-P-107334 Assigned To OCR

Due Date: 05/29/2019 10:00 AM Eastern

Instructions:

Instructions:

Please review and edit/comment with track changes the attached draft report.

Background: The attached draft report, entitled "Use of Cell-Site Simulator Technology," responds to a requirement contained in the Joint Explanatory Statement (Conference Report) accompanying the Fiscal Year 2019 DHS Appropriations Act (P.L. 116-6). That report requires DHS to "update the Committees on the implementation and oversight of DHS Policy Directive 047-02, related to cell site simulators by the Department and its state and local partners."

Note: This report was produced using previously-cleared information provided by the subject DHS Components and draws heavily from the language of DHS's previous report on this topic.

Due Dates:

Non-Lead:

HSI Taskings: NLT 10AM - 5/29/2019

OCFO Taskings: NLT 10AM - 5/29/2019

Policy Taskings: NLT 10AM - 5/29/2019

Reviewer:

OCR Taskings: NLT 10AM - 5/29/2019

OPLA Taskings: NLT 2PM - 5/29/2019

OES is not responsible for coordinating or consolidating Program Office responses.

The lead program office must reconcile all ICE intra-agency comments and/or questions prior to closing their task bar.

Thank you.

Best,

(b)(6); (b)(7)(C)

Taskings Analyst
Office of the Executive Secretariat
Office of the Director
U.S. Immigration and Customs Enforcement
202.732. [redacted]

(b)(7)(E) [redacted] ice.dhs.gov

Thank you.

From: (b)(6); (b)(7)(C)
Sent: 23 Nov 2020 21:50:59 +0000
To: (b)(6); (b)(7)(C)
Subject: Venntel Congressional files for redaction
Attachments: VENNTEL Congressional Letter.pdf
Importance: High

Good afternoon (b)(6); (b)(7)(C)

We received this request and wanted to see if you have received this or were aware of this or any request from the committee on this issue?

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Sent: Monday, November 9, 2020 11:24 AM
To: HSI Records Disclosure Unit (b)(7)(E) @ice.dhs.gov>
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: Venntel Congressional files for redaction
Importance: High

To Whom it May Concern:

(b)(5)

At your earliest convenience, please let me know what information you will need or if there are any additional steps that need to be taken by HSI Intel relating to the Congressional inquiry. Please see attached the Venntel Congressional letter for reference and a summary of the recommendations for redactions below.

Summary

(b)(5)

- **Third-Party public disclosure request/Personally identifiable** - 8 emails containing 104 documents were categorized as Personally Identifiable
- **Law Enforcement Sensitive (LES) Information/Investigative Emails** - 39 emails containing 20 documents were categorized as Investigative emails
- **Law Enforcement Sensitive (LES) Information/Tradecraft Methods and Techniques** - 107 emails containing 82 documents were categorized as Tradecraft Methods and Techniques

- **(Law Enforcement Sensitive LES) Technical-** 90 emails containing 106 documents were categorized as Technical emails. (b)(7)(E)

(b)(7)(E)

The communications were between Venntel and HSI offices (mostly Intel offices/ Field and HQ).

The data is stored on SharePoint and is located here:

(b)(7)(E)

Thank you.

(b)(6); (b)(7)(C)

Section Chief
Enterprise Services Division
Technology, Innovation, and Project Management Section
U.S. Immigration and Customs Enforcement
Homeland Security Investigations/Intelligence
Unclass (b)(6); (b)(7)(C) @ice.dhs.gov
HSDN: (b)(6); (b)(7)(C) @dhs.gov
Office (202) 732 (b)(6);
Cell (202) 46 (b)(7)(C)

"If everyone is thinking alike, then somebody isn't thinking."

Congress of the United States
Washington, DC 20515

June 24, 2020

Mr. Chris Gildea
President
Venntel, Inc.
2201 Cooperative Way, Suite 600
Herndon, VA 20171

Dear Mr. Gildea:

We are investigating the collection and sale of sensitive mobile phone location data that reveals the precise movements of millions of American adults, teens, and even children. We seek information about your company's provision of consumer location data to federal government agencies for law enforcement purposes without a warrant and for any other purposes, including in connection with the response to the coronavirus crisis.

The vast majority of Americans carry cell phones with apps capable of collecting precise location information 24 hours a day, 7 days a week. This location-tracking raises serious privacy and security concerns. As Chief Judge Roberts wrote in the *Carpenter* opinion, "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."¹ This location data can reveal where we go and with whom we associate, tracking us in our homes, at the doctor, or at church.²

With Americans installing contact-tracing apps as part of the effort to limit the spread of COVID-19, it has become increasingly important to make sure that the American public has a full understanding of who is collecting their location data, how it may be provided to the government, and what the government is doing with it.

It was recently reported that a contact-tracing app recommended to residents by the governors of North Dakota and South Dakota was sending location data to a third party—in violation of promises made to users.³ According to that third party, the data was not used; nevertheless, this example shows that Americans may increasingly be unwittingly handing over their location data to unknown third party data brokers such as Venntel. There are limited restrictions on how this data may be sold to and used by the federal government.

¹ *Carpenter v. United States*, 138 S.Ct. 2206 (2018).

² *The Government Uses 'Near Perfect Surveillance' Data on Americans*, New York Times (Feb. 7, 2020) (online at www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html).

³ *One of the First Contact-Tracing Apps Violates Its Own Privacy Policy*, Washington Post (May 21, 2020) (online at www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/).

In February, the Wall Street Journal reported that Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) purchased consumers' location data from Venntel and used it without a warrant to identify, locate, and arrest migrants.⁴ According to the report:

The Trump administration has bought access to a commercial database that maps the movements of millions of cellphones in America and is using it for immigration and border enforcement. ... The location data is drawn from ordinary cellphone apps, including those for games, weather and e-commerce, for which the user has granted permission to log the phone's location.⁵

Federal spending records indicate that the Drug Enforcement Agency (DEA), Federal Bureau of Investigation (FBI), and Internal Revenue Service (IRS) also may have obtained data or data services from your company.⁶ Furthermore, federal, state, and local governments reportedly are using or considering the use of cell phone location data to track the spread of the coronavirus.⁷

The Supreme Court has held that the government must obtain a warrant before agencies can obtain location data from wireless phone companies and technology companies like Facebook and Google. By acting as an intermediary in the sale of this data, your company may be selling data to the government that it otherwise would need a warrant to compel, impacting the privacy of millions of people, including vulnerable populations like children.⁸

Consumers often do not understand that popular apps for weather, travel, shopping, and other purposes—which may have legitimate needs for location data—may be selling this data to brokers.⁹ An investigation in 2018 by the New York Times uncovered 75 companies that were

⁴ *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall Street Journal (Feb. 7, 2020) (online at www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600).

⁵ *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall Street Journal (Feb. 7, 2020) (online at www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600).

⁶ *USASpending.gov* (accessed June 22, 2020).

⁷ *U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus*, Washington Post (Mar. 17, 2020) (online at www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/); *Government Tracking How People Move Around in Coronavirus Pandemic*, Wall Street Journal (Mar. 28, 2020) (online at www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202);

⁸ See 18 U.S.C. § 2702.

⁹ *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, New York Times (June 12, 2019) (online at www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html); Federal Trade Commission, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers* (Dec. 5, 2013) (online at www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived).

buying and selling mobile app-derived location data.¹⁰ Location-targeted advertising sales are predicted to reach an estimated \$27 billion this year.¹¹

The scale of this data collection is staggering. For example, Venntel's reported parent company, Gravy Analytics,¹² has revealed that it collects location data from software "embedded within tens of thousands of apps."¹³ According to its website, Gravy Analytics "processes billions of pseudonymous mobile location signals every day from millions of mobile devices."¹⁴ Despite claims that anonymization protects privacy, computer scientists and journalists repeatedly have demonstrated the ease with which individuals in purportedly anonymized data sets may be identified.¹⁵

Reports also indicate that location data is vulnerable to hacking and that this data could lead to individuals being targeted for commercial or political purposes, stalking, or discrimination.¹⁶ In 2017, the Massachusetts Attorney General reached a settlement with a company that targeted advertisements to "abortion-minded women" entering reproductive health facilities and methadone clinics in multiple states.¹⁷ Media reports have also identified companies targeting advertisements to people in emergency rooms¹⁸ and dialysis centers.¹⁹ In

¹⁰ *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, New York Times (Dec. 10, 2018) (online at www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html).

¹¹ *Location Targeted Mobile Advertising Spending in the United States from 2016 to 2023*, Statista (Nov. 8, 2019) (online at www.statista.com/statistics/274837/local-and-national-mobile-us-ad-spending-since-2009/).

¹² *Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones*, Protocol (Mar. 5, 2020) (online at www.protocol.com/government-buying-location-data).

¹³ Gravy Analytics, *Location Data & COVID-19* (online at gravyanalytics.com/covid-19/) (accessed June 22, 2020).

¹⁴ Gravy Analytics, *Our Data* (online at gravyanalytics.com/our-data/) (accessed June 22, 2020).

¹⁵ *Twelve Million Phones, One Dataset, Zero Privacy*, New York Times (Dec. 19, 2019) (online at www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html).

¹⁶ *A Location-Sharing Disaster Shows How Exposed You Really Are*, Wired (May 19, 2018) (online at www.wired.com/story/locationsmart-securus-location-data-privacy/); *Hundreds of Apps Can Empower Stalkers to Track Their Victims*, New York Times (May 19, 2018) (online at www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html); *Catholics in Iowa Went to Church. Steve Bannon Tracked Their Phones*, ThinkProgress (July 19, 2019) (online at <https://thinkprogress.org/exclusive-steve-bannon-geofencing-data-collection-catholic-church-4aaeacd5c182/>); Senate Committee on Commerce, Science, and Transportation, Ranking Member Maria Cantwell, *The State of Online Privacy and Data Security* (Nov. 2019) (online at www.cantwell.senate.gov/imo/media/doc/The%20State%20of%20Online%20Privacy%20and%20Data%20Security.pdf).

¹⁷ *Firm Settles Massachusetts Probe over Anti-abortion Ads Sent to Phones*, Reuters (Apr. 4, 2017) (online at www.reuters.com/article/us-massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSKBN1761PX).

¹⁸ *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, New York Times (Dec. 10, 2018) (online at www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html).

¹⁹ *Political Campaigns Know Where You've Been. They're Tracking Your Phone*, Wall Street Journal (Oct. 10, 2019) (online at www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889).

2019, the Los Angeles City Attorney brought a lawsuit against the Weather Channel and its parent company, IBM, which sell data collected from the Weather Channel app's 45 million users. The City Attorney alleged the companies deceptively collected, shared, and profited from the location information of millions of American consumers.²⁰

In February 2020, the Federal Communications Commission (FCC) fined the four major wireless carriers, Verizon, AT&T, T-Mobile, and Sprint, for selling location data without the knowledge or consent of their subscribers. In issuing the fines, the FCC described the sensitivity of location data and its potential for abuse:

The precise physical location of a wireless device is an effective proxy for the precise physical location of the person to whom that phone belongs at that moment in time. Exposure of this kind of deeply personal information puts those individuals at significant risk of harm—physical, economic, or psychological. For consumers who have job responsibilities in our country's military, government, or intelligence services, exposure of this kind of information can have serious national security implications.²¹

For all of these reasons, please provide the following information and documents by July 8, 2020, for the period from January 1, 2016, to the present:

1. For each provision of goods or services to a federal agency by your company:
 - a. documents sufficient to show the nature and purpose of the product or service provided and any use case or justification provided by the purchasing agency;
 - b. documents sufficient to show any actions that Venntel or its suppliers take to obtain the consent of the individuals whose location and other data is provided to or accessed by the agency;
 - c. all documents relating to any restrictions on how the agency may use the product or service, including whether the agency may share information with other federal or state government agencies and whether Venntel and the agency entered into a nondisclosure agreement regarding the agency's use of Venntel's services;
 - d. documents sufficient to show Venntel's revenue from the sale or provision of the goods or services;
 - e. copies of all contracts or agreements relating to the sale or provision of the goods or services;
2. All correspondence between Venntel and any employee, official, or representative of any federal department, federal agency, or executive branch office;

²⁰ *Los Angeles Accuses Weather Channel App of Covertly Mining User Data*, New York Times (Jan. 3, 2019) (online at www.nytimes.com/2019/01/03/technology/weather-channel-app-lawsuit.html).

²¹ *See, e.g.*, Federal Communications Commission, *Notice of Apparent Liability for Forfeiture and Admonishment*, T-Mobile (Feb. 28, 2020) (online at <https://docs.fcc.gov/public/attachments/FCC-20-27A1.pdf>).

3. A list of all customers who purchase, license, or access location data from Venntel or any Venntel subsidiary. For each customer, please provide the following:
 - a. documents sufficient to show the nature and purpose of the product or service provided;
 - b. documents sufficient to show any actions that Venntel or its suppliers take to obtain the consent of the individuals whose location and other data is provided to or accessed by the customer;
 - c. all documents relating to any restrictions on how the customer may use the product or service;
 - d. copies of all contracts or agreements relating to the sale or provision of the goods or services;
 - e. for any foreign entity, detail the steps Venntel has taken to seek and obtain export licenses for these sales;
4. A description of any COVID-19 related efforts that Venntel is involved in, including:
 - a. any COVID-19-related apps from which Venntel collects or has collected data;
 - b. any documents related to the provision of goods or services to federal agencies, state governments, local law enforcement, and foreign entities, related to monitoring or mitigating the COVID-19 pandemic; and
5. Documents sufficient to show the specific location data that Venntel collects, other information it collects (*e.g.*, Advertising ID, wireless information, web search history, phone or demographic information), and how is it paired or combined with location data;
6. Documents sufficient to show the number of individuals from whom Venntel collects location data;
7. Information indicating how long Venntel keeps user data, regardless of whether it is anonymized;
8. Documents sufficient to identify all sources from which Venntel and its upstream suppliers have received consumer location and other data which it provides to any government agency, and the specific type of data collected from each source. For each source, please provide documents sufficient to show the following:
 - a. the amount paid by Venntel to receive location data from that source;
 - b. copies of all contracts or written agreements with that source;
9. Documents sufficient to show all measures Venntel or its upstream suppliers take, if any, to ensure the anonymity of users whose data is collected by Venntel;

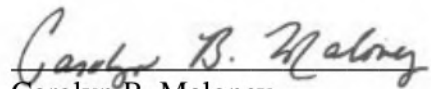
10. Documents sufficient to show all steps Venntel takes, contractually or otherwise, to ensure that its customers do not attempt to re-identify anonymized data provided to them;
11. A description of how Venntel ensures that all data it buys and sells, licenses, or provides access to was obtained from individuals who consented to the collection of, use of, sale of, or sale of access to their data, including to federal agencies and law enforcement agencies;
12. A description of any data security practices and policies Venntel uses to ensure that location data is not accessed without authorization;
13. A description of each instance in which Venntel's location data has been breached or accessed without authorization; and
14. Copies of all policies and procedures related to the collection, use, license, or sale of location data, including with respect to data security, data privacy, user consent, and anonymization.

The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

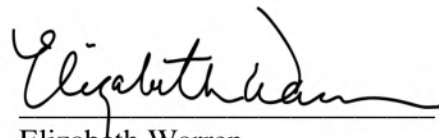
An attachment to this letter provides additional instructions for responding to this request. If you have any questions regarding this request, please contact Committee staff at (202) 225-5051, Senator Warren's staff at (202) 224-4543, or Senator Wyden's staff at (202) 224-5244.

Thank you for your attention to this important matter.

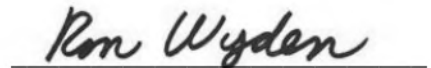
Sincerely,



Carolyn B. Maloney
Chairwoman
House Committee on Oversight and Reform



Elizabeth Warren
United States Senator



Ron Wyden
United States Senator



Mark DeSaulnier
Member of Congress

Enclosure

cc: The Honorable Jim Jordan, Ranking Member,

Mr. Chris Gildea

Page 7

House Committee on Oversight and Reform

Responding to Oversight Committee Document Requests

1. In complying with this request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. Produce all documents that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party.
2. Requested documents, and all documents reasonably related to the requested documents, should not be destroyed, altered, removed, transferred, or otherwise made inaccessible to the Committee.
3. In the event that any entity, organization, or individual denoted in this request is or has been known by any name other than that herein denoted, the request shall be read also to include that alternative identification.
4. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, thumb drive, or secure file transfer) in lieu of paper productions.
5. Documents produced in electronic format should be organized, identified, and indexed electronically.
6. Electronic document productions should be prepared according to the following standards:
 - a. The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - b. Document numbers in the load file should match document Bates numbers and TIF file names.
 - c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - d. All electronic documents produced to the Committee should include the following fields of metadata specific to each document, and no modifications should be made to the original metadata:

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,

INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,
BEGATTACH.

7. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, zip file, box, or folder is produced, each should contain an index describing its contents.
8. Documents produced in response to this request shall be produced together with copies of file labels, dividers, or identifying markers with which they were associated when the request was served.
9. When you produce documents, you should identify the paragraph(s) or request(s) in the Committee's letter to which the documents respond.
10. The fact that any other person or entity also possesses non-identical or identical copies of the same documents shall not be a basis to withhold any information.
11. The pendency of or potential for litigation shall not be a basis to withhold any information.
12. In accordance with 5 U.S.C. § 552(d), the Freedom of Information Act (FOIA) and any statutory exemptions to FOIA shall not be a basis for withholding any information.
13. Pursuant to 5 U.S.C. § 552a(b)(9), the Privacy Act shall not be a basis for withholding information.
14. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
15. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) every privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, addressee, and any other recipient(s); (e) the relationship of the author and addressee to each other; and (f) the basis for the privilege(s) asserted.
16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (by date, author, subject, and recipients), and explain the circumstances under which the document ceased to be in your possession, custody, or control.
17. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents that would be responsive as if the date or other descriptive detail were correct.

18. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data, or information not produced because it has not been located or discovered by the return date shall be produced immediately upon subsequent location or discovery.
19. All documents shall be Bates-stamped sequentially and produced sequentially.
20. Two sets of each production shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2105 of the Rayburn House Office Building.
21. Upon completion of the production, submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control that reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, data, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, communications, electronic mail (email), contracts, cables, notations of any type of conversation, telephone call, meeting or other inter-office or intra-office communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, mail, releases, electronic

message including email (desktop or mobile device), text message, instant message, MMS or SMS message, message application, or otherwise.

3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information that might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neutral genders.
4. The term “including” shall be construed broadly to mean “including, but not limited to.”
5. The term “Company” means the named legal entity as well as any units, firms, partnerships, associations, corporations, limited liability companies, trusts, subsidiaries, affiliates, divisions, departments, branches, joint ventures, proprietorships, syndicates, or other legal, business or government entities over which the named legal entity exercises control or in which the named entity has any ownership whatsoever.
6. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual’s complete name and title; (b) the individual’s business or personal address and phone number; and (c) any and all known aliases.
7. The term “related to” or “referring or relating to,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with, or is pertinent to that subject in any manner whatsoever.
8. The term “employee” means any past or present agent, borrowed employee, casual employee, consultant, contractor, de facto employee, detailee, fellow, independent contractor, intern, joint adventurer, loaned employee, officer, part-time employee, permanent employee, provisional employee, special government employee, subcontractor, or any other type of service provider.
9. The term “individual” means all natural persons and all persons or entities acting on their behalf.