NATIONAL TARGETING CENTER

U.S. Customs and Border Protection

NTC Identifies Possible Human/Narcotic Smuggler in (b) (7)(E), (b) (7)(A) [redacted]

BOTTOM LINE UP FRONT

Using open source advertisement ID tools and tradecraft, NTC's (b) (7)(E) [redacted]) identified a possible distributor and/or smuggler operating at a stash hous [redacted] Homeland Security Investigation (HSI) case.

(b) (7)(E), (b) (7)(A) [redacted]

BACKGROUND

(b) (7)(E), (b) (7)(A) [redacted]

ORDER FOR SUPPLIES OR SERVICES

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER: 9/24/2019
2. CONTRACT NO. (if any): HSHQDC 12 D 00013
3. ORDER NO.: 70B04C19F00000802
4. REQUISITION/REFERENCE NO.: 0020111511
5. ISSUING OFFICE (Address correspondence to):
DHS Customs & Border Protection
Customs and Border Protection
1300 Pennsylvania Ave, NW
Procurement Directorate NP 1310
Washington DC 20229

6. SHIP TO:
a. NAME OF CONSIGNEE: See Attached Delivery Schedule
b. STREET ADDRESS:
c. CITY:
d. STATE:
e. ZIP CODE:
f. SHIP VIA:

7. TO:
a. NAME OF CONTRACTOR: PANAMERICA COMPUTERS, INC.
b. COMPANY NAME:
c. STREET ADDRESS: 1386 BIG OAK RD.
d. CITY: LURAY
e. STATE: VA
f. ZIP CODE: 22835

8. TYPE OF ORDER
☐ a. PURCHASE Reference Your . Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
☒ b. DELIVERY Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA:

10. REQUISITIONING OFFICE
(b)(6) (b)(7)(C)

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
☒ a. SMALL ☐ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED ☒ e. HUBZone
☐ f. SERVICE-DISABLED VETERAN-OWNED ☐ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM ☐ h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)

12. F.O.B. POINT: Origin

13. PLACE OF
a. INSPECTION:
b. ACCEPTANCE:

14. GOVERNMENT B/L NO.:

15. DELIVER TO F.O.B POINT ON OR BEFORE (Date): 09/25/2020

16. DISCOUNT TERMS: Within 30 days Due net

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Accpt
10	(b) (7)(E)	(b) (7)(E)	EA	(b) (7)(E), (b) (4)		
20	(b) (7)(E)		EA			
30	Venntel		EA			
40	Venntel - TASPD		EA			
50	Vennte (b) (7)(E) - TASPD		EA			

18. SHIPPING POINT:
19. GROSS SHIPPING WEIGHT:
20. INVOICE NO.:

17(h)TOT. (Cont. pages): $0.00

21. MAIL INVOICE TO:
a. NAME: DHS Customs & Border Protection Commercial Accounts Sect.
b. STREET ADDRESS (or P.O. Box): 6650 Telecom Drive, Suite 100
c. CITY: Indianapolis
d. STATE: IN
e. ZIP CODE: 46278

SEE BILLING INSTRUCTIONS REVERSE

17(i) GRAND TOTAL: $1,068,317.18

22. UNITED STATES OF AMERICA BY (Signature): (b)(6) (b)(7)(C)

23. NAME (Typed): (b) (6), (b) (7)(C)
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

Federal Tax Exempt ID: 72-0408780

Emailing Invoices to CBP. **Do not mail or email invoices to CBP. Invoices must be submitted via the IPP website, as detailed under Electronic Invoicing and Payment Requirements in the attached terms and conditions.**

NOTES:

This Firm Fixed Price delivery order, 70B04C19F00000802, is issued against the Department of Homeland Security FirstSource II HSHQDC 12 D 00013 fo [redacted] Venntel Software in support of the Targeting and Analysis Systems Program Directorate (TASPD). The Statement of Work will be provided with the Award Distribution email.

Reference Bid # 566657146, dated 8/15/2019, from Unison Buy # 984602.

The period of performance will be 9/27/2019 9/25/2020.

CONTRACTING OFFICER'S REPRESENTATIVE

Name: [redacted]
Address: 5971 Kingstowne Village Pkwy.
5th floor mailroom
Alexandria, Virginia 22315
Tel. #: [redacted]
Fax. #:
Email: [redacted]@cbp.dhs.gov

IPP APPROVER

Nam [redacted]
Address: 5971 Kingstowne Village Pkwy.
5th floor mailroom
Alexandria, Virginia 22315
Tel. #: [redacted]
Fax. #:
Email: [redacted]@cbp.dhs.gov

IPP.gov in accordance with Section 10.5 of the SOW.

All Terms and Conditions of the FirstSource II Contract HSHQDC 12 D 00013 are in full force and effect.

ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: 70B04C19F00000802

I.1 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	(b) (7)(E) [redacted]	[redacted]	EA	(b) (7)(E), (b) (4) [redacted]	
20			EA		
30	Venntel	(b) (7)(E) [redacted]	EA		
40	Venntel - TASPD		EA		
50	Vennt (b) (7)(E) [redacted] - TASPD		EA		

Total Funded Value of Award: **$1,068,317.18**

I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	(b) (7)(E) [redacted]	(b) (7)(E), (b) (4) [redacted]
20		
30		
40		
50		

I.3 DELIVERY SCHEDULE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 5971 Kingstown Village Parkway Alexandria, VA 22315	10	(b) (7)(E) [redacted]	09/25/2020
	20		09/25/2020
	30		09/25/2020
	40		09/25/2020
	50		09/25/2020

I.4 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):
www.acquisition.gov

I.5 CONTRACT TYPE (OCT 2008)

This is a Firm Fixed Price Contract.

[End of Clause]

I.6 PERIOD OF PERFORMANCE (MAR 2003)

The period of performance of this contract shall be from 9/27/2019 through 9/25/2020.

[End of Clause]

I.7 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or condition of the contract. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

[End of Clause]

I.8 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: https://www.ipp.gov.

Under this contract, the following documents are required to be submitted as an attachment to the IPP*:*

-_____

-_____

-_____

-_____

-_____

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(End of Clause)

I.9 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

[End of Clause]

Department of Homeland Security
Customs & Border Protection (CBP)
Provisions Statement for Third Party Software Licenses and Maintenance

1.0 GENERAL INFORMATION AND SCOPE

U.S. Customs and Border Protection (CBP) requires the purchase of software in support of the National Targeting Center (NTC) and the Targeting and Analysis Systems Program Directorate (TASPD). This software is in support of pilots for th (b) (7)(E) [redacted].

The purpose of this firm-fixed price contract is for the contractor to provide the following software:

Item Description	Quantity
(b) (7)(E) *In accordance with the attached Bill of Materials	(b) (7)(E) [redacted]
(b) (7)(E) *In accordance with the attached Bill of Materials	
Venntel *In accordance with the attached Bill of Materials	
Vennt (b) (7)(E) *In accordance with the attached Bill of Materials	

The Contractor shall provide technical support, codes for fixes, access to product documentation and any updates.

1.1 PERIOD OF PERFORMANCE

The period of performance will be 9/27/19-9/25/20.

1.2 PLACE OF PERFORMANCE

Place of performance will be at government facilities.

2.0 SPECIFIC TASKS

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

2.3 VENNTEL

In accordance with this SOW, Venntel will provide the following:

1. Capability: Access to Venntel global mobile location database via the portal.
2. Support: Customer support and account management. Venntel will provide 2 hours of training per license.

3.0 TYPE OF CONTRACT

Customs and Border Protection will award a firm fixed price contract.

4.0 INVOICING AND PAYMENT

ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: https://www.ipp.gov.

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(b) In accordance with FAR 32.904(b), the CO, in conjunction with the COR and NFC, will determine whether the invoice is proper or improper within seven (7) days of receipt. Improper invoices will be returned to the contractor within seven (7) days of receipt.

REVIEW AND APPROVAL REQUIREMENTS

(a) To constitute a proper invoice, invoices shall include, at a minimum, all the items required in FAR 32.905.

The minimum requirements are:

Name and address of the contractor.

Invoice date and invoice number.

Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number.

Description, quantity, unit of measure, unit price, and extended price of supplies delivered or services performed.

Shipping and payment terms (e.g. shipment number and date of shipment, discount for prompt payment terms). Bill of lading number and weight of shipment will be shown for shipments on Government bills of lading.

Name and address of contractor official to whom payment is to be sent (must be the same as that in the contract or in a proper notice of assignment).

Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.

Taxpayer identification number (TIN).

Electronic funds transfer (EFT) banking information.

Any other information or documentation required by the contract (e.g. evidence of shipment).

(b) Supplemental documentation required for review and approval of invoices, at the written direction of the contracting officer, may be submitted directly to either the contracting officer, or the contracting officer's representative. Contractors shall submit all supplemental invoice documentation along with the original invoice.

(c) Invoices that fail to provide the information required by the Prompt Payment clause (FAR 52.232-25) may be rejected by the Government and returned to the contractor.

5.0 POINT OF CONTACT

CONTRACTING OFFICER'S REPRESENTATIVE

Name [redacted]

Address: 5971 Kingstowne Village Pkwy.
5th floor mailroom
Alexandria, Virginia 22315

Tel. #: [redacted]

Fax. #:

Email: [redacted]@cbp.dhs.gov

IPP APPROVER

Name: [redacted]

Address: 5971 Kingstowne Village Pkwy.
5th floor mailroom

Alexandria, VA 22315
Tel. #: (b) (6), (b) (7)(C)
Fax. #:
Email: [redacted]@cbp.dhs.gov

6.0 Personally Identifiable Information (PII)

When a contractor, on the behalf of CBP, handles Sensitive PII data, stores and transmits, the contractor will Accredit (ATO) this information system to the High, High, Moderate (HHM) FIPS level.

7.0 DHS CLAUSES

Enterprise Architecture (EA) Compliance

The Offeror shall ensure that the design conforms to the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) Enterprise Architecture (EA), the DHS and CBP Technical Reference Models (TRM), and all DHS and CBP policies and guidelines (such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture - Technical Framework), as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA).

The Offeror shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model, as described in their respective EAs. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles, as reflected by the hardware, software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software, or infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process (to include a trade study with no less than four alternatives, one of which reflecting the status quo and another reflecting multi-agency collaboration). The DHS/CBP TRM/standards profile will be updated as TIs are resolved.

All developed solutions shall be compliant with the Homeland Security (HLS) EA.
All IT hardware and software shall be compliant with the HLS EA.
Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines. Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

Compliance with DHS Security Policy Terms and Conditions

All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

Encryption Compliance

If encryption is required, the following methods are acceptable for encrypting sensitive information:

1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
2. National Security Agency (NSA) Type 2 or Type 1 encryption.
3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

<u>DHS Enterprise Architecture Compliance</u>

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

4. All developed solutions and requirements shall be compliant with the HLS EA.
5. All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
6. Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise

Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

7. Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
8. Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

Required Protections for DHS Systems Hosted in Non-DHS Data Centers

Security Authorization

A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of the DHS information system.

At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the COTR for entry into the DHS' Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by the DHS POA&M Management Process. Contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments.

On a periodic basis, the DHS and its Components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the

contractor under these clauses. Evaluation could include, but it not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture to the best of its ability and to the satisfaction of the DHS COTR. Areas of consideration could include:

1) Use of multi-tier design (separating web, application and data base) with policy enforcement between tiers
2) Compliance to DHS Identity Credential Access Management (ICAM)
3) Security reporting to DHS central control points (i.e. the DHS Security Operations Center (SOC) and integration into DHS Security Incident Response
4) Integration into DHS Change Management (for example, the Infrastructure Change Control Board (ICCB) process)
5) Performance of activities per continuous monitoring requirements

Continuous Monitoring

The contractor shall participate in DHS' Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that the DHS determines acceptable. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the contractor shall implement the following processes:

1. Asset Management
2. Vulnerability Management
3. Configuration Management
4. Malware Management
5. Log Integration
6. Security Information Event Management (SIEM) Integration
7. Patch Management
8. Providing near-real-time security status information to the DHS SOC

Specific Protections

Specific protections that shall be provided by the contractor include, but are not limited to the following:

Security Operations

The Contractor shall operate a SOC to provide the security services described below. The Contractor shall support regular reviews with the DHS Information Security Office to coordinate and synchronize the security posture of the contractor hosting facility with that of the DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The contractor staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the contractor staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the contractor facility SOC shall adhere to the incident response plan.

Computer Incident Response Services

The Contractor shall provide Computer Incident Response Team (CIRT) services. The contractor shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The contractor shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The contractor shall notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration.

Firewall Management and Monitoring

The Contractor shall provide firewall management services that include the design, configuration, implementation, maintenance, and operation of all firewalls within the hosted DHS infrastructure in accordance with DHS architecture and security policy. The contractor shall provide all maintenance to include configuration, patching, rule maintenance (add, modify, delete), and comply with DHS' configuration management / release management requirements when changes are required. Firewalls shall operate 24x7x365. Analysis of the firewall logs shall be reported to DHS COTR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Intrusion Detection Systems and Monitoring

The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be reported to DHS COTR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Physical and Information Security and Monitoring

The Contractor shall provide a facility using appropriate protective measures to provide for physical security. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to DHS IT assets. DHS IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office.

Vulnerability Assessments

The Contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

Anti-malware (e.g., virus, spam)

The Contractor shall design, implement, monitor and manage to provide comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COTR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Patch Management

The Contractor shall perform provide patch management services. The contractor shall push patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches that are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.

Log Retention

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

Personal Identification Verification (PIV) Credential Compliance

Authorities:

HSPD-12 ―Policies for a Common Identification Standard for Federal Employees and Contractors‖
OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors"
OMB M-06-16 ―Acquisition of Products and Services for Implementation of HSPD-12‖
NIST FIPS 201 ―Personal Identity Verification (PIV) of Federal Employees and Contractors‖
NIST SP 800-63 ―Electronic Authentication Guideline‖
OMB M-10-15 ―FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management‖

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.
Procurements for software products or software developments shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.
If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

Section 508 Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at

https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

Item that contains Information and Communications Technology (ICT): CND PAIG Tools
Applicable Exception: N/A **Authorization #:** N/A
Applicable Functional Performance Criteria: All functional performance criteria apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.
Applicable requirements for electronic content features and components (including Internet and Intranet website; Electronic reports):
Applicable requirements for software features and components (including Software infrastructure; Service Offerings): All WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application
Applicable requirements for hardware features and components: Does not apply
Applicable support services and documentation: All requirements apply

2. When providing installation, configuration or integration services for ICT, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

3. When providing maintenance upgrades, substitutions, and replacements to ICT, the contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution or replacement. Prior to acceptance, the contractor shall provide an Accessibility Conformance Report (ACR). The ACR should be created using the on the Voluntary Product Accessibility Template Version 2.1 or later. The template can be located at https://www.itic.org/policy/accessibility/vpat

4. When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.

5. When developing or modifying web and software ICT, the contractor shall demonstrate Section 508 conformance by providing Section 508 test results based on the versions of the DHS Trusted Tester Methodology currently approved for use, as defined at https://www.dhs.gov/compliance-test-processes. The contractor shall use testers who are certified by DHS on how to use the DHS Trusted Tester Methodology (e.g "DHS Certified Trusted Testers") to conduct accessibility

testing. Information on how testers can become certified is located at https://www.dhs.gov/publication/trusted-tester-resources.

6. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.

Acceptance Criteria

1. Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the contractor to provide the following:
    - Accessibility test results based on the required test methods.
    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation of core functions that cannot be accessed by persons with disabilities.
    - Documentation on how to configure and install the ICT Item to support accessibility.
    - Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content where applicable).
2. Before accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

ISO (Information Security) COMPLIANCE

- **Information Security Clause:**

"All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD4300.1, *Information Technology Systems Security Program* and *4300A Sensitive Systems Handbook."*

- **Interconnection Security Agreements**

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

HSAR Clauses

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions*. As used in this clause

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available in any medium and from any source that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations

thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.
"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:
(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)
Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.
(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.
(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide

copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.
(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.
(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.
(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security*

Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at

the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.
(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:
(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract

award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access

to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

Interconnection Security Agreement (ISA)

INTERCONNECTION SECURITY AGREEMENTS TERMS AND CONDITIONS

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

Required Protections for DHS Systems Hosted in Non-DHS Data Centers

SECURITY AUTHORIZATION

A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of the DHS information system.

At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the COTR for entry into the DHS' Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by the DHS POA&M Management Process. Contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments.

On a periodic basis, the DHS and its Components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these clauses. Evaluation could include, but it is not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

ENTERPRISE SECURITY ARCHITECTURE TERMS AND CONDITIONS

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture to the best of
its ability and to the satisfaction of the DHS COTR. Areas of consideration could include:

1. Use of multi-tier design (separating web, application and data base) with policy enforcement between tiers
2. Compliance to DHS Identity Credential Access Management (ICAM)
3. Security reporting to DHS central control points (i.e. the DHS Security Operations Center (SOC) and integration into DHS Security Incident Response
4. Integration into DHS Change Management (for example, the Infrastructure Change Control Board (ICCB) process)
5. Performance of activities per continuous monitoring requirements

CONTRACTOR EMPLOYEE ACCESS (SEP 2012)

Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
(b) “Information Technology Resources” include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.
(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.
(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, and insubordination, incompetence, or security concerns.
(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.
(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.
(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer’s Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.
(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as

approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.
(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).
(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.
(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:
(1) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
(2) The waiver must be in the best interest of the Government.
(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

- **System Security documentation appropriate for the SELC status**

Security Certification/Accreditation

CBP Program Offices shall provide personnel (System Owner and Information System Security Officers) with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with the current version of the DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems Security Policies and Procedures Handbook HB-1400-05, and all applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series). During all SELC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools. An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO. While the ISSO performs security functions, the System Owner is always responsible for information system security (4300A). System owners shall include information security requirements in their capital planning and investment control (CPIC) business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS information system. System

owners or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.

Disaster Recovery Planning & Testing – Hardware

If the system owner requires a robust DR solution (full redundancy and failover capabilities (for near zero downtime) then the funded DR solution must match the production environment like-for-like. This solution would also include additional software licenses, hardware, firmware and storage for the DR environment.
The system owner or program office must also include travel, per diem and approximately 16 over the core hours for travel to recovery facilities twice per fiscal year for system administrators, DBA's, end users or testers
If the system owner requires a moderate DR solution that would provide a working environment that is capable of handling their mission essential functions then they can fund a scaled down solution which should still take into consideration additional hardware, software licenses, and storage for the DR environment.
The system owner or program office is still responsible for the costs associated with testing their DR solution; however, for a scaled down solution, it may be possible to leverage or share staff already designated to participate in DR activities.
If the system owner only requires a low DR solution then the system owner or program office can use internal resources to perform a table-top exercise, which generally does not require travel, additional hardware or software licenses.

- **Monitoring/reviewing contractor security requirements clause**

Security Review and Reporting

(a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.
(b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the organization of the DHS Office of the Chief Information Officer, Office of Inspector General, the CBP Chief Information Security Officer, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/CBP data or the function of computer systems operated on behalf of DHS/CBP, and to preserve evidence of computer crime.

- **Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information**

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems Security* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

OMB-M-07-18 FDCC

In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.

Engineering Platforms

- **Common Enterprise Services (CES)** Deliver the systems, infrastructure, and operational capabilities to fully implement the three service levels defined as part of the DHS/CBP Common Enterprise Services and support DHS Component use of those services. This includes the build out and integration of all required services and infrastructure, which must include the Single Sign-on Portal and CBP Enterprise Services Bus (ESB), required for the CES. Capabilities shall be designed to the DHS standard operating architecture (SOA), transportable between DHS data centers (CBP National Data Center, Stennis, and DHS 2nd data center).

- **Single Sign-on Portal** Design, build, and operate a single sign-on Portal - consistent with DHS' enterprise portal solution (for which ICE is the steward) - to provide a common point of access, with a single sign-on capability to existing applications and to provide the infrastructure for integrating diverse internal and/or external information and transactional resources. This includes the migration of the current ACE Portal to the Single Sign-on Portal as rapidly as feasible.

ITP (Infrastructure Transformation Program) COMPLIANCE

All back-end system hardware and software shall be hosted in the DHS Enterprise Data Center unless Component provides a migration plan or obtains an approved waiver from DHS CIO.

All DHS Wide Area Network circuits must be part of the OneNet architecture unless a waiver is approved by DHS CIO.

- **Help Desk and Operations Support**

The contractor shall provide third tier reporting for trouble calls received from the Help Desk, the DHS Task Manager, or the users. The Contractor shall respond to the initiators of trouble calls as by receiving telephonic notifications of problems, resolving them, or directing them to the proper technical personnel for resolution. Problems that cannot be resolved immediately or with the requirements of the performance standards are to be brought to the attention of the DHS Task Manager. The Contractor shall document notification and resolution of problems in Remedy.

- **Interfacing**

As requested by the COTR, assistance in consolidating all systems with the DHS Consolidated Data Center. Resources to be consolidated with the DHS Consolidated Data Center, for each system will be determined by the COTR.

DHS GEOSPATIAL INFORMATION SYSTEM COMPLIANCE

All geospatial implementations shall comply with the policies and requirements set forth for the DHS Geospatial Information Infrastructure (GII). This shall include submission to the Enterprise Architecture Board, or their designee, for review and approval of insertion of hardware, software, services, appliances, and/or structural metadata into the Homeland Security Enterprise Architecture (HLS EA).

TRANSITION PLAN

The DHS CIO has established portfolio targets for the IT infrastructure that include production system consolidation at a DHS data center, and transition to OneNet. The contractor must be prepared to support CBP government leads, within the purview of this task order, to provide any required transition planning or program execution, associated with meeting the agreed to transition timeline, as directed by Government personnel. This includes the following types of tasking's:

- Coordination with Government representatives
- Review, evaluation and transition of current support services
- Transition of historic data to new contractor system
- Government-approved training and certification process

- Transfer of all necessary business and/or technical documentation
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable debriefing and personnel out-processing procedures

Portfolio Review

Screening/Watchlist/Credentialing

Includes all activities that support the tracking and monitoring of travelers, conveyances and cargo crossing U.S. borders, traffic pattern analysis, database (Federal, State, and Local) linking and querying, managing status verification and tracking systems. Different investments and systems may support distinct screening and watchlist activities for people, cargo, and tangible goods. Credentialing encompasses all activities that determine a person's eligibility for a particular license, privilege, or status, from application for the credential through issuance, use, and potential revocation of the issued credential.

Supply Chain Risk Management
Supply Chain Risks result from adversarial exploitation of the organizations, people, activities, information, resources, or facilities that provide hardware, software, or services. These risks can result in a loss of confidentiality, integrity, or availability of information or information systems. A compromise to even minor system components can lead to adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
The following should be included in all hardware and software requests to ensure the confidentiality, integrity, and availability of government information:
Supply Chain Risk Management Terms and Conditions:
The Contractors supplying the Government hardware and software shall provide the manufacture's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state and/or domain of registration and DUNs number of those suppliers must also be provided.

Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.
The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software. The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.

The Supply Chain Risk Management Plan shall address the following elements:

1. *How risks from the supply chain will be identified,*
2. *What processes and security measures will be adopted to manage these risks to the system or system components, and*
3. *How the risks and associated security measures will be updated and monitored.*

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Technical Representative (COTR) 30 days post award.

The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents an unacceptable risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standards certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the Contracting Officer (CO). Contractors shall only provide Original Equipment Manufacturers (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

The Contractor shall be excused from using new OEM (i.e. "grey market," previously used) components only with formal Government approval. Such components shall be procured from their original genuine source and have the components shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e. until the "end of life."). Software updates and patches must be made available to the government for all products procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the US Government as having the authority to examine them.

This transit process shall minimize the number of times en route components undergo a change of custody and make use tamper-proof or tamper-evident packaging for all

shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.
The Contractor is fully liable for all damage, deterioration, or losses incurred during shipment and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

Subject: FW: Invitatio (b) (6) Venntel Team - Introductions @ Wed Jul 15, 2020 1pm - 1:30pm (ED (b)(6) (b)(7)(C) @cbp.dhs.gov)

Start: Wed 7/15/2020 1:00 PM
End: Wed 7/15/2020 1:30 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: (b)(6) (b)(7)(C) n behalf (b) (6) @venntel.com

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

-----Original Appointme (b) (6)
From (b) (6) @venntel.co @venntel.com>
Sent: Friday, July 10, 20 1:38 PM
T (b) (6) @venntel.com (b) (6) (b) (6), (b) (7)(C)
Subject: Invitatio (b)(6) (b)(7)(C) Venntel Team - Introductions @ Wed Jul 15, 2020 1pm - 1:30pm (EDT)
(b)(6) (b)(7)(C) @cbp.dhs.gov)
When: Wednesday, July 15, 2020 1:00 PM-1:30 PM (UTC-05:00) Eastern Time (US & Canada).
Where:

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

You have been invited to the following event.

(b)(6) (b)(7)(C) Venntel Team - Introductions

When

Wed Jul 15, 2020 1pm 1:30pm Eastern Time - New York

Calendar

(b)(6) (b)(7)(C) [redacted] @cbp.dhs.gov

Who

- (b) (6) [redacted] @venntel.com - organizer
- (b) (6) [redacted]
- (b) (6) [redacted]
- (b)(6) (b)(7)(C) [redacted] @cbp.dhs.gov

more details »

(b) (6) [redacted] is inviting you to a scheduled Zoom meeting.

Topi (b) (6) [redacted] Personal Meeting Room

Join Zoom Meeting

(b)(7)(E) [redacted]

Meeting I (b)(7)(E) [redacted]

Passwor (b)(7)(E) [redacted]

One tap mobile

(b)(7)(E) [redacted] US (Chicago)

US (New York)

Dial by your location

(b)(7)(E)

(Chicago)

(New York)

(Germantown)

(Tacoma)

(Houston)

(San Jose)

(San Jose)

(b)(7)(E)

Meeting I

Passwor (b)(7)(E)

Find your local number:

(b)(7)(E)

Goin (b)(6) (b)(7)(C) @cbp.dhs.gov)? **Yes** - **Maybe** - **No** more options »

Invitation from Google Calendar

You are receiving this courtesy email at the accou (b)(6) (b)(7)(C) @cbp.dhs.gov because you are an attendee of this event.

To stop receiving future updates for this event, decline this event. Alternatively you can sign up for a Google account at https://www.google.com/calendar/ and control your notification settings for your entire calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. Learn More.

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.

invite.ics

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

Venntel Team - Introductions

(b)(7)(E)

CONFIRMED

PRODID
-//Google Inc//Google Calendar 70.9054//EN

Version
2.0

CALSCALE
GREGORIAN

METHOD
REQUEST

Start Date/Time
20200715T170000Z

End Date/Time
20200715T173000Z

DTSTAMP
20200710T173753Z

ORGANIZER (C (b)(6) @venntel.com)
mailt (b)(6) @venntel.com

UID
68nf8aleb2ofrset2rpa54ru9n@google.com

Attendee **mail (b) (6) @venntel.com**
Role REQ-PARTICIPANT
RSVP TRUE

Attendee **mail (b) (6) venntel.com**
Role REQ-PARTICIPANT
RSVP TRUE

Attendee **mailto (b)(6) (b)(7)(C) @cbp.dhs.gov**
Role REQ-PARTICIPANT
RSVP TRUE

Attendee **mailt (b)(6) @venntel.com**
Role REQ-PARTICIPANT
RSVP TRUE

X-MICROSOFT-CDO-OWNERAPPTID
(b)(7)(E)

CREATED
20200710T173751Z

Description

(b) (6) is inviting you to a scheduled Zoom meeting.

Topi (b) (6) Personal Meeting Room

Join Zoom Meeting
(b)(7)(E)

Meeting ID (b)(7)(E)
Password (b)(7)(E)
One tap m
(b)(7)(E) US (Chicago)
US (New York)

Dial by your location
(b)(7)(E) (Chicago)
(New York)
(Germantown)
(Tacoma)
(Houston)
(San Jose)
(San Jose)
Meeting I (b)(7)(E)
Passwor (b)(7)(E)
Find your s://zoom.us/u/aAicjz40P

-::~:~::~::~:~::-
Please do not edit this section of the description.

View your event at
(b)(7)(E)

-::~:~::~::~:~::-

Last Modified
20200710T173751Z

Location

Sequence Number
0

Status
CONFIRMED

Summary
(b) (6) Venntel Team - Introductions

Time Transparency
OPAQUE

Subject: Invitati (b)(6) (b)(7)(C) Venntel Team - Introductions @ Wed Jul 15, 2020 1pm - 1:30pm (ED (b)(6) (b)(7)(C) @cbp.dhs.gov)

Start: Wed 7/15/2020 1:00 PM
End: Wed 7/15/2020 1:30 PM

Recurrence: (none)

Meeting Status: Accepted

Organizer: (b) (6) @venntel.com

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

-----Original Appointment-----
Fro (b) (6) @venntel.com <bo@venntel.com>
Sent: Friday, July 10, 2020 1:38 PM
T (b) (6) @venntel.c (b) (6) (b) (6), (b) (7)(C)
Subject: Invitatio (b)(6) (b)(7)(C) (b) (7)(C) Venntel Team - Introductions @ Wed Jul 15, 2020 1pm - 1:30pm (EDT) @cbp.dhs.gov)
When: Wednesday, July 15, 2020 1:00 PM-1:30 PM (UTC-05:00) Eastern Time (US & Canada).
Where:

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

You have been invited to the following event.

(b)(6) (b)(7)(C) Venntel Team - Introductions

When

Wed Jul 15, 2020 1pm 1:30pm Eastern Time - New York

Calendar

(b)(6) (b)(7)(C) @cbp.dhs.gov

Who

- (b) (6) @venntel.com - organizer
- (b) (6)
- (b) (6)
- (b)(6) (b)(7)(C) @cbp.dhs.gov

more details »

(b) (6) is inviting you to a scheduled Zoom meeting.

Top (b) (6) Personal Meeting Room

Join Zoom Meeting

(b)(7)(E)

Meeting I (b)(7)(E)

Passwor (b)(7)(E)

One tap mobile

(b)(7)(E) US (Chicago)

US (New York)

Dial by your location

(b)(7)(E) US (Chicago)

US (New York)

US (Germantown)

US (Tacoma)

US (Houston)

US (San Jose)

US (San Jose)

Meeting I (b)(7)(E)

Passwor (b)(7)(E)

Find your local number:

(b)(7)(E)

Goin (b)(6) (b)(7)(C) @cbp.dhs.gov)? **Yes** - **Maybe** - **No** more options »

Invitation from Google Calendar

You are receiving this courtesy email at the accou (b)(6) (b)(7)(C) @cbp.dhs.gov because you are an attendee of this event.

To stop receiving future updates for this event, decline this event. Alternatively you can sign up for a Google account at https://www.google.com/calendar/ and control your notification settings for your entire calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. Learn More.

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.

invite.ics

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

Venntel Team - Introductions

20200715T170000Z
CONFIRMED

PRODID
-//Google Inc//Google Calendar 70.9054//EN

Version
2.0

CALSCALE
GREGORIAN

METHOD
REQUEST

Start Date/Time
20200715T170000Z

End Date/Time
20200715T173000Z

DTSTAMP
20200710T173753Z

ORGANIZER (C (b) @venntel.com)
mailto (b) @venntel.com

UID
68nf8aleb2ofrset2rpa54ru9n@google.com

Attendee **mailt (b) (6) @venntel.com**
Role REQ-P ICIPANT
RSVP TRUE

Attendee **mailt (b) (6) @venntel.com**
Role REQ-PARTICIPANT
RSVP TRUE

Attendee **mailt** (b) (6), (b) (7)(C) **@cbp.dhs.gov**
Role REQ-PARTICIPANT
RSVP TRUE

Attendee **mail (b) (6) @venntel.com**
Role REQ-PARTICIPANT
RSVP TRUE

X-MICROSOFT-CDO-OWNERAPPTID
(b)(7)(E)

CREATED
20200710T173751Z

Description

(b) (6) is inviting you to a scheduled Zoom meeting.

Top (b) (6) Personal Meeting Room

Join Zoom Meeting

(b)(7)(E)

Meeting I (b)(7)(E)
Passwor (b)(7)(E)
One tap mobile

(b)(7)(E) US (Chicago)
US (New York)

Dia (b)(7)(E)
US (Chicago)
US (New York)
US (Germantown)
US (Tacoma)
US (Houston)
US (San Jose)
US (San Jose)

Meeting I (b)(7)(E)
Password (b)(7)(E)
Find your l ber (b)(7)(E)

-::~:~::~::~:~::-
Please do not edit this section of the description.

View your event at

(b)(7)(E)

-::~:~::~::~:~::-

Last Modified

20200710T173751Z

Location

Sequence Number

0

Status

CONFIRMED

Summary

(b)(6) (b)(7)(C) Venntel Team - Introductions

Time Transparency

OPAQUE

From: DOSTAL, JON
Sent: Friday, July 10, 2020 4:49 PM
To: (b) (6) @venntel.com
Subject: Accepted: Invitati (b)(6) (b) Venntel Team - Introductions @ Wed Jul 15, 2020 1pm - 1:30pm (ED (b)(6) (b)(7)(C) @cbp.dhs.gov)

Bid Details for Bid #: 565063147

Report generated 09/06/2018 17:05:39 ET

Buy Information

Buyer Organization: DHS Customs and Border Protection (CBP)
Buyer Re (b)(6) (b)(7)(C)
Buy Description: Infrastructure Equipment for Tri Cities Global Enrollment Center
Internal Description: Infrastructure Equipment for Tri Cities Global Enrollment Center
Solicitation No.: 20107297
Start Date / Time: 08/30/2018 08:19 ET
End Date / Time: 09/05/2018 18:00 ET

Set-Aside Requirement: HUBZone Small Business
Contract Vehicle: DHS FirstSource II
Seller Community: DHS FirstSource II – HUBZone Socioeconomic Category

FedBizOpps Solicitation: No
FAC: 2005-100
Purchase Description: Brand Name or Equal
Specialized Buy Type: No
Award Type: Purchase Order or Delivery Order
Seller Attachments: Attachments Optional
Seller Question Deadline: No Seller Question Deadline Set - None

Target Price

Total Target Price: $772,500.00 - Target Price is Active
Bid Decrement: $100

Suggested Sellers

Company Name	Phone	Sales Rep	Email
No sellers added			

Category

PSC 70 -- Information Technology (ADP) Equipment (Including Firmware), Software, Supplies and Support Equipment

Sub-category

PSC 7050 -- IT Components

NAICS

541690 -- Other Scientific and Technical Consulting Services

Bid Details

Company Information

Bid Description:	Misc Softwar (b)(7)(E) (b)(7)(E) Venntel
Company Name:	PANAMERICA COMPUTERS, INC. [DUNS: 166669742]

Seller Information

Sales Rep Name:	(b) (6)
Address:	1386 Big Oak Rd
City:	Luray
State:	VA

© 2001 - 2018 FedBid, Inc. All rights reserved.

Address:	1386 BIG OAK RD
City:	LURAY
State:	VA
Zip Code:	22835
Phone:	TBD
Fax:	
Duns No:	166669742
Cage Code:	301Q5
Tax ID:	541689773
FedBid Buy No:	946089
Socio-Economic Classification:	Small Business , Women-Owned Business , 8(A) , Minority-Owned Business , HUBZone Small Business , Small Disadvantaged Business , Women-Owned Small Business , Economically Disadvantaged Women-Owned Small Business

Zip Code:	22835
Phone:	(b) (6) [redacted]
Fax:	
Email:	

CPARS Contractor Rep

Name:	(b) (6) [redacted]
Phone Number:	
Email:	

SAM Information

This information was obtained from the System for Award Management (SAM.gov) on 09/06/2018. Any due diligence required by any applicable parties, statutes or regulations should be used in accordance with FAR Subpart 42.15.

SAM Name:	PANAMERICA COMPUTERS, INC.
SAM DUNS:	166669742
Active Exclusion:	No
Registration Status:	Active
Expiration Date:	11/17/2018
Active Exclusion:	No

✓ **The vendor complies with all terms listed by the Buyer.**

Delivery

30 Day(s) - **Required** (No. of calendar days after receipt of order (ARO) by which Buyer requires Seller to deliver)

Shipping Address

See Statement of Work

Contract

Notice: This is a contract Buy. Before accepting, please verify that Line Item pricing does not exceed applicable contract pricing.

Contract No.:	HSHQDC-12-D-00013
Contract Owner:	PCi Tec
Contract Expiration Date:	09/16/2018
Delivery Days:	30

Seller Attachment(s)

No.	Document Name	Document Size
No Seller Attachment(s)		

© 2001 - 2018 FedBid, Inc. All rights reserved.

Line Item(s)

Notice: This is a contract Buy. Before accepting, please verify that Line Item pricing does not exceed applicable contract pricing.

Item No.	Description	Qty	Unit Price	Ext. Price
001	Requested Specification: (SEE SOW FOR DETAILS) Seller Line Item Details: (b) (7)(E)	(b) (7)(E)	(b) (7)(E), (b) (4)	
002	Requested Specification: (SEE SOW FOR DETAILS) Seller Line Item Details: (b) (7)(E)	(b) (7)(E)		
003	Requested Specification: (SEE SOW FOR DETAILS) Seller Line Item Details: (b) (7)(E)	(b) (7)(E)		
004	Requested Specification: (SEE SOW FOR DETAILS) Seller Line Item Details: **Manufacturer:** Venntel **Part Number:** Mobile device Ad-tech **Description:** Venntel: Mobile device's Ad-tech ID data	(b)		

Price Summary

Total Price: **$1,467,869.90**

Bidding Requirements

Seller Attachment(s): In addition to providing pricing through the marketplace, Sellers have the OPTION to include certain non-pricing information as document(s) attached to their Bid, so they are received no later than the closing date and time of this Buy. Pricing will not be accepted if it is included in the attachment(s). Attachment(s) can total no more than 20 MB, whether multiple files or one file, and may be zipped to decrease their size. A Seller's failure to comply with these terms may result in its Bid being determined to be non-responsive. The attachment(s) should include the following non-pricing information: Please attach additional specification for technical evaluation.

DHS FirstSource II Bids Only: Seller shall ONLY bid on this opportunity if they are able to provide commercially-available IT commodities, solutions, and value-added reseller (VAR) services per the requirements established in the Delivery Order solicitation. Seller shall adhere to all terms and conditions stated in their respective DHS FirstSource II IDIQ contract, AS WELL AS any additionally imposed through the Delivery Order solicitation - provided they do not contradict those executed by the former. Both the status of the Seller (i.e. its ability to conduct business with the Federal Government) and the status of the Seller's IDIQ contract shall be in an ACTIVE state at the time a bid is submitted.

Brand Name or Equal: The Buyer is allowing Sellers to submit bids for alternate items, provided those items meet all of the salient physical, functional, or performance characteristics specified by this solicitation. Sellers

© 2001 - 2018 FedBid, Inc. All rights reserved.

Bidding Requirements

MUST enter exactly what they are bidding (including make, model and description) into the blank description field in order for the bid to be considered. The Buyer will evaluate 'equal' items on the basis of information furnished by the Seller or identified in the bid and reasonably available to the Buyer. The Buyer is not responsible for locating or obtaining any information not identified in the Bid.

Minimum Bid Decrement is $100: The Buyer is requiring that any rebid must be lower than the 'current bid price' by this amount. The reduction is based on the total order and must be satisfied within the rebid minimum.

Purchase Order or Delivery Order: Buyer intends to issue award using a purchase order or delivery order. Bids from Sellers unable to accept purchase orders or delivery orders will not be considered for award.

Set-Aside Requirement: This solicitation is a HUBZone Small Business set-aside and only qualified Sellers can bid.

Use of FedBid: Buyers and Sellers agree to conduct this transaction through FedBid in compliance with the FedBid Terms of Use. Failure to comply with the below terms and conditions may result in offer being determined as non-responsive.

Evaluation Criteria/Basis of Award: Sellers understand that the Marketplace ranks all Bids by price; however, pursuant to applicable acquisition regulations and/or departmental guidelines, Buyers may use criteria other than price to evaluate offers. Accordingly, please note that, unless otherwise specified in the Buy Terms, below, to the extent required by applicable regulations and/or guidelines, award will be made to the responsible Seller whose offer conforming to the solicitation will be most advantageous to the Buyer on the basis of price, technical capability, delivery, and past performance.

Question Submission: Interested offerors must submit any questions concerning the solicitation at the earliest time possible to enable the buyer to respond. Questions can be submitted by using the 'Questions & Responses' link. Questions not received within a reasonable time prior to close of the solicitation may not be considered.

Default Terms: Unless otherwise specified in the Buy Terms, below, Bid must be good for 30 calendar days after close of Buy and shipping must be free on board (FOB) destination CONUS (Continental U.S.)

Buy Terms

Name	Criteria
Pricing Instructions	Unless the Buyer indicates otherwise within a particular line item description, each Seller shall include in its online Bid individual pricing for all required line items in order to be considered for award (i.e., Do not use the Included in another line item function when pricing each line item). If a line item cannot be separately priced, you must notify the buyer through the FedBid Submit a Question feature regarding which line item(s) should be included in which other line item(s) and request reposting. Failure to comply with this term may result in the Bid being determined to be non-responsive.
Equipment Condition	New Equipment ONLY; NO remanufactured or "gray market" items. All items must be covered by the manufacturer's warranty.
Offer Period	Bid MUST be good for 30 calendar days after close of Buy.
Shipping Condition	Shipping must be free on board (FOB) destination CONUS (Continental U.S.), which means that the seller must deliver the goods on its conveyance at the destination specified by the buyer, and the seller is responsible for the cost of shipping and risk of loss prior to actual delivery at the specified destination.
SAM Requirement	This solicitation requires registration with the System for Award Management (SAM) prior to award, pursuant to applicable regulations and guidelines. Registration information can be found at www.sam.gov.
ORCA Requirement	ORCA Requirement - Company must be registered on Online Representations and Certifications Application (ORCA) before an award could be made to them. If company is not registered with ORCA, they may do so by going to ORCA web site at https://orca.bpn.gov/.
Delivery Requirement	No partial shipments are permitted unless specifically authorized at the time of award.

© 2001 - 2018 FedBid, Inc. All rights reserved.

Buy Terms

Name	Criteria
Delivery Of Order	Delivery must be made within 30 days or less after receipt of order (ARO). The offeror must provide within its offer the number of days - not to exceed 30 - required to make delivery after it receives a purchase order from the buyer. Unless otherwise noted.
Q&A Instructions	Q&A -Please submit all questions by using the 'Submit a Question' button. This buy will then be reposted with Q&A based on the questions that come in (if applicable).
Award Criteria	Award Criteria-An award will be made to a responsive offeror (who submits all required submissions on time), whose past performance does not pose a risk to the Government, and whose offer is the Lowest Price Technically Acceptable (LPTA). An offer is technically acceptable if its technical capabilities conform to the Government's Statement of Work or listed specs whichever is applicable to the buy.
Supplemental Bid Information	Supplemental Bid Information In addition to providing pricing at www.FedBid.com for this solicitation, each Offeror must provide any required, NON-PRICING responses (e.g. technical proposal, representations and certifications, etc.) so that they are received no later than the closing date and time for this solicitation. Submissions can be sent to clientservices@fedbid.com.
For Exact Match Only Commodity Buys	For Exact Match Only Commodity Buys- NO SUBSTITUTIONS, EXACT MATCH ONLY. The vendor may not substitute any item/service listed on this order without prior written approval from the DHS/CBP Contracting Officer. No other individual is authorized, either verbally or in writing to change part numbers, manufacturer, quantity, delivery dates, or any other specifications of this RFQ. Items/services that do not conform to descriptions and part numbers found in this RFQ will be rejected at the time of delivery causing a return at the vendor's expense.
For Exact Match Services Buys Only	For Exact Match Services Buys Only- In order for a sellers bid to be 'responsive' and considered for award, the seller is REQUIRED to document exactly how they intend to meet the requirements of the SOW. They shall document statement detailing the service for evaluation. Failure to do this may be cause for termination. This information is REQUIRED in order for a sellers bid to be deemed 'responsive' and to be considered for award.
For Buys other than Exact Match:	For all buys other than Exact Match Sellers MUST document what they are bidding for evaluation for award. Sellers must include, extended specs and/or manufacturer name and part numbers (if applicable). Failure to do this may be cause for termination. This information is REQUIRED in order for a sellers bid to be deemed 'responsive' and to be considered for award. FAR 52.211-6
IPP Clause	In accordance with the IPP clause; ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016), payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: https:// www.ipp.gov. Contractor assistance with IPP enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131. If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

© 2001 - 2018 FedBid, Inc. All rights reserved.

ORDER FOR SUPPLIES OR SERVICES

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER: 09/27/2018
2. CONTRACT NO. (if any): HSHQDC 12 D 00013
3. ORDER NO.: 70B04C18F00001214
4. REQUISITION/REFERENCE NO.: 0020107297
5. ISSUING OFFICE (Address correspondence to):
DHS Customs & Border Protection
Customs and Border Protection
1300 Pennsylvania Ave, NW
Procurement Directorate NP 1310
Washington DC 20229

6. SHIP TO:
a. NAME OF CONSIGNEE: See Attached Delivery Schedule
b. STREET ADDRESS:
c. CITY:
d. STATE:
e. ZIP CODE:
f. SHIP VIA:

7. TO:
a. NAME OF CONTRACTOR: PANAMERICA COMPUTERS, INC.
b. COMPANY NAME:
c. STREET ADDRESS: 1386 BIG OAK RD.
d. CITY: LURAY
e. STATE: VA
f. ZIP CODE: 22835

8. TYPE OF ORDER
☐ a. PURCHASE Reference Your BID# 565063147 . Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
☒ b. DELIVERY Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA:

10. REQUISITIONING OFFICE
(b) (6), (b) (7)(C)

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
☒ a. SMALL ☐ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED ☒ e. HUBZone
☐ f. SERVICE-DISABLED VETERAN-OWNED ☐ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM ☐ h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)

12. F.O.B. POINT: Not applicable

13. PLACE OF
a. INSPECTION:
b. ACCEPTANCE:

14. GOVERNMENT B/L NO.:

15. DELIVER TO F.O.B POINT ON OR BEFORE (Date): 09/26/2019

16. DISCOUNT TERMS: Within 30 days Due net

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Accpt
10	(b) (7)(E)	(b) (7)(E)	EA	(b) (7)(E), (b) (4)		
20			EA			
30			EA			
40	Venntel	(b) (7)(E)	EA	(b) (7)(E), (b) (4)		
50	Venntel		EA			
60	(b) (7)(E)	(b) (7)(E)	EA	(b) (7)(E), (b) (4)		
70			EA			

18. SHIPPING POINT:
19. GROSS SHIPPING WEIGHT:
20. INVOICE NO.:

17(h) TOT. (Cont. pages): $0.00

21. MAIL INVOICE TO:
SEE BILLING INSTRUCTIONS REVERSE
a. NAME: DHS Customs & Border Protection Commercial Accounts Sect.
b. STREET ADDRESS (or P.O. Box): 6650 Telecom Drive, Suite 100
c. CITY: Indianapolis
d. STATE: IN
e. ZIP CODE: 46278

17(i) GRAND TOTAL: $1,467,869.90

22. UNITED STATES OF AMERICA BY (Signature): (b)(6) (b)(7)(C)
TITLE: CONTRACTING/ORDERING OFFICER

Federal Tax Exempt ID (b) (3) (A)

Emailing Invoices to CBP. **Do not mail or email invoices to CBP. Invoices must be submitted via the IPP website, as detailed under Electronic Invoicing and Payment Requirements in the attached terms and conditions.**

NOTES:

This Firm Fixed Price delivery order, 70B04C18F00001214, is issued against the Department of Homeland Security FirstSource II Contract HSHQDC-12-D-00013 for Counter Networ (b) (7)(E) ools in support of the Targeting and Analysis Systems Program Directorate (TASPD). The Statement of Work will be provided with the Award Distribution email.

Reference Bid # 565063147 dated September 5, 2018, from FedBid Buy # 946089.

The Period of Performance for 70B04C18F00001214 is from September 27, 2018 - September 26, 2019.

The Contracting Officer's Representative for this order is:
Name (b)(6) (b)(7)(C)
Address: 5971 Kingstowne Village Pkwy.
5th floor mailroom
Alexandria, Virginia 22315
Tel. #: (b) (6), (b) (7)(C)
Fax. #:
Email: @cbp.dhs.gov

Invoices shall be sent to:
IPP.gov in accordance with Section 10.5 of the SOW.

All Terms and Conditions of the FirstSource II Contract HSHQDC-12-D-00013are in full force and effect.

ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: 70B04C18F00001214

I.1 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	(b) (7)(E)		EA	(b) (7)(E), (b) (4)	
20			EA		
30			EA		
40	Venntel	(b) (7)(E)	EA	(b) (7)(E), (b) (4)	
50	Venntel		EA		
60	(b) (7)(E)	(b) (7)(E)	EA	(b) (7)(E), (b) (4)	
70			EA		

Total Funded Value of Award: **$1,467,869.90**

I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	(b) (7)(E)	(b) (7)(E), (b) (4)
20		
30		
40		
50		
60		
70		

I.3 DELIVERY SCHEDULE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 5971 Kingstown Village Parkway Alexandria, VA 22315	10	(b) (7)(E)	09/26/2019
	20		09/26/2019
	30		09/26/2019
	40	(b) (7)(E)	09/26/2019
	50		09/26/2019
	60	(b) (7)(E)	09/26/2019
	70		09/26/2019

I.4 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an “I agree” click box or other comparable mechanism (e.g., “click-wrap” or “browse-wrap” agreements), execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(End of clause)

I.5 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)

(a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

I.6 52.204-22 ALTERNATIVE LINE ITEM PROPOSAL (JAN 2017)

I.7 3052.205-70 ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASES (SEP 2012) ALTERNATE I (SEP 2012)

(a) The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

(b) All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

(End of clause)

I.8 3052.212-70 CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (SEP 2012)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

[The Contracting Officer should either check the provisions and clauses that apply or delete the provisions and clauses that do not apply from the list. The Contracting Officer may add the date of the provision or clause if desired for clarity.]

(a) Provisions.

[ ] 3052.209-72 Organizational Conflicts of Interest.

[ ] 3052.216-70 Evaluation of Offers Subject to An Economic Price Adjustment Clause.

[ ] 3052.219-72 Evaluation of Prime Contractor Participation in the DHS Mentor Protégé Program.

(b) Clauses.

[ ] 3052.203-70 Instructions for Contractor Disclosure of Violations.

[ ] 3052.204-70 Security Requirements for Unclassified Information Technology Resources.

[ ] 3052.204-71 Contractor Employee Access.

[ ] Alternate I

[ ] 3052.205-70 Advertisement, Publicizing Awards, and Releases.

[ ] 3052.209-73 Limitation on Future Contracting.

[ ] 3052.215-70 Key Personnel or Facilities.

[ ] 3052.216-71 Determination of Award Fee.

[ ] 3052.216-72 Performance Evaluation Plan.

[ ] 3052.216-73 Distribution of Award Fee.

[ ] 3052.219-70 Small Business Subcontracting Plan Reporting.

[ ] 3052.219-71 DHS Mentor Protégé Program.

[ ] 3052.228-70 Insurance.

[ ] 3052.236-70 Special Provisions for Work at Operating Airports.

[ ] 3052.242-72 Contracting Officer's Technical Representative.

[ ] 3052.247-70 F.o.B. Origin Information.

[ ] Alternate I

[ ] Alternate II

[ ] 3052.247-71 F.o.B. Origin Only.

[ ] 3052.247-72 F.o.B. Destination Only.

(End of clause)

I.9 52.224-3 PRIVACY TRAINING, ALTERNATE I (DEVIATION)

(a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) *Circular A-130, Managing Federal Information as a Strategic Resource*).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who--

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will –

(1) Have a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

I.10 PERIOD OF PERFORMANCE (MAR 2003)

The period of performance of this contract shall be from 09/27/2018 through 09/26/2019.

[End of Clause]

I.11 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or condition of the contract. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

[End of Clause]

I.12 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: https://www.ipp.gov.

Under this contract, the following documents are required to be submitted as an attachment to the IPP*:*

-_____

-_____

-_____

-_____

-_____

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(End of Clause)

I.13 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

[End of Clause]

I.14 SECURITY PROCEDURES (OCT 2009)

A. Controls

1. The Contractor shall comply with the U.S. Customs and Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.

2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor shall comply with all security policies contained in CBP Handbook 1400-05C, Information Systems Security Policies and Procedures Handbook.

3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Management Directive (MD) 4300.1, Information Technology Systems Security Program and DHS 4300A, Sensitive Systems Handbook.

4. All Contractor employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Technical Representative (COTR). The COTR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Internal Affairs, Security Management Division (IA/SMD) should be notified if building access is revoked.

5. All Contractor employees must be registered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COTR. The Contractor shall provide timely start information to the CO/COTR or designated government personnel to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COTR or designated government personnel shall provide the Contractor with instructions for receipt of CTS registration information. Additionally, the CO/COTR shall immediately notify IA/SMD of the contractor's departure/separation.

6. The Contractor shall provide employee departure/separation date and reason for leaving to the CO/COTR in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the Contractor to provide timely notification of employee departure/separation in accordance with the contract

requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

B. Security Background Investigation Requirements

1. In accordance with DHS Management Directive (MD) 11055, Suitability Screening Requirements for Contractors, Part VI, Policy and Procedures, Section E, Citizenship and Residency Requirements, contractor employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status. A waiver may be granted, as outlined in MD 11055, Part VI, Section M (1).

2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with MD 11055, Part VI, Section E (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in MD 11055, Part VI, Section M (2)

3. Provided the requirements of DHS MD 11055 are met as outlined in paragraph 1, above, contractor employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the employee's access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor employee's life, including employment, education, residences, police and court inquires, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPI).

4. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated BI or SSBI that meets federal investigation standards.. For employee candidates needing a BI for this contract, the Contractor shall require the applicable employees to submit information and documentation requested by CBP to initiate the BI process.

5. Background Investigation information and documentation is usually submitted by completion of standard federal and agency forms such as Questionnaire for Public Trust and Selected Positions or Questionnaire for National Security Positions; Fingerprint Chart; Fair Credit Reporting Act (FCRA) form; Criminal History Request form; and Financial Disclosure form. These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.

6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of contractor employees who successfully complete the CBP BI or SSBI process. Failure of any contractor employee to obtain and maintain a favorably adjudicated BI or SSBI shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COTR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel contractor employees, the Contractor shall propose a qualified replacement employee candidate to the COTR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COTR shall approve or disapprove replacement employees. Continuous failure to provide contractor employees who meet CBP BI or SSBI requirements may be cause for termination of the contract.

C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.

2. The CO/COTR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.

3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the

solicitation/contract. The Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.

4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.

5. Upon completion of this contract, the Contractor shall return all sensitive information used in the performance of the contract to the CO/COTR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

D. Notification of Contractor Employee Changes

1. The Contractor shall notify the CO/COTR via phone, facsimile, or electronic transmission, immediately after a personnel change become known or no later than five (5) business days prior to departure of the employee. Telephone notifications must be immediately followed up in writing. Contractor's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.

2. The Contractor shall notify the CO/COTR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. The CO/COTR will notify the Office of Information and Technology (OIT) Information Systems Security Branch (ISSB) of the proposed change. If a security clearance is required, the CO/COTR will notify IA/SMD.

E. Non-Disclosure Agreements

When determined to be appropriate, Contractor employees are required to execute a non-disclosure agreement (DHS Form 11000-6) as a condition to access sensitive but unclassified information.

[End of Clause]

I.15 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:

   a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).

   b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.

   c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self certification, by public records check, or other reference checks conducted in the normal course of business.

2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition*:* *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

[End of Clause]

U.S. Department of Homeland Security
U.S. Customs and Border Protection
Office of Field Operations

National Targeting Center

(b) (7)(E)

(b) (7)(E)

User Group – All CBP tactical targeting/analytical units, intelligence support cells, special operations groups, protective details and enforcement units such a (b) (7)(E)

Requirements (b) (7)(E)
(b) (7)(E)

Specifications (b) (7)(E) accessed via web based portal. Training support (in-person and web).

(b) (5), (b) (7)(E)

(b) (7)(E)

Contract Vehicle - Acquisition through Thundercat (with access to First Source II)

[1] OFO NTC (CND Ops Teams a (b) (7)(E) an (b) (7)(E) Field Office, USBP (b) (7)(E) NBCC

U.S. Department of Homeland Security
U.S. Customs and Border Protection
Office of Field Operations

National Targeting Center

(b) (7)(E)

(b) (7)(E)

User Group – All CBP tactical targeting units, intelligence support cells, special operations groups, protective details and enforcement units such as: National Targeting Center (NTC) Analysts and Operators, Tactical Analytical Units (TAUs), USBP Sector Intel Units (SIUs), Office of Intelligence – Current Intel (OI-CI) Analysts

(b) (7)(E)

Specifications (b) (7)(E) Training support (in-person and web).

(b) (5), (b) (7)(E)

U.S. Department of Homeland Security
U.S. Customs and Border Protection
Office of Field Operations
National Targeting Center

(b) (7)(E)

(b) (7)(E)

Contract Vehicle - Acquisition through Thundercat (with access to First Source II)

Price Quote for DHS CBP - NTC – June 13, 2019

Quote good for 120 days

Customer:
DHS CBP – TASPD
[redacted] (b)(6) (b)(7)(C)
Washington, DC 20528

Venntel Ad Hoc Data Services (SKU: S-001)	
# of Special Data Projects	Annual fe [redacted] Special Projects
[redacted]	[redacted] (b) (4)
Ad Hoc Special Data Projects will b [redacted] (b) (7)(E) per project	

Venntel Contact Information:
[redacted] (b) (6)
(b) (6) @venntel.com
(b) (6)

Venntel Inc.
2201 Cooperative Way
Suite 600
Herndon, VA 20171
DUNS: 08060176

All Pricing is Business Confidential

Reverse Auction Results for: 984602

Report generated 08/16/2019 10:23:08 ET

Buy Information

Buyer Organization: DHS Customs and Border Protection (CBP)
Buyer Re [redacted] (b)(6) (b)(7)(C)
Buy Descriptio [redacted] (b)(7)(E) Venntel Software
Internal Descriptio [redacted] (b)(7)(E) Venntel Software 20111511
Solicitation No.: 20111511
Start Date / Time: 08/08/2019 15:23 ET
End Date / Time: 08/15/2019 17:00 ET

Set-Aside Requirement: HUBZone Small Business
Contract Vehicle: DHS FirstSource II
Seller Community: DHS FirstSource II HUBZone Socioeconomic Category

FedBizOpps Solicitation: No
FAC: 2019-03
Purchase Description: Brand Name Only (Exact Match)
Specialized Buy Type: No
Award Type: Purchase Order or Delivery Order
Seller Attachments: Attachments Required
Seller Question Deadline: No Seller Question Deadline Set - None
Reverse Auction: Yes

Your Bid Summary

Total Sellers Notified: 6
Total Sellers Bidding: 1
Number of Bids: 2
Number of No Bids: 2

Target Price

Total Target Price: $1,038,744.35 - Target Price is Active
Bid Decrement: $100

Suggested Sellers

Company Name	Phone	Sales Rep	Email
No sellers added			

Category

PSC 70 -- Information Technology (ADP) Equipment (Including Firmware), Software, Supplies and Support Equipment

Sub-category

PSC 7050 -- IT Components

NAICS

541519 -- Other Computer Related Services

Delivery

30 Day(s) - **Required** (No. of calendar days after receipt of order (ARO) by which Buyer requires Seller to deliver)

Shipping Address

See Statement of Work

© 2019 Unison Marketplace Inc., All rights reserved.

Line Item(s)

Item No.	Description	Qty	Unit
001	(b) (7)(E) SEE SPEC SHEET	(b) (7)(E)	EA
002	(b) (7)(E) SEE SPEC SHEET	(b) (7)(E)	EA
003	Venntel: Mobile device's Ad-tech ID data SEE SPEC SHEET	(b) (7)(E)	EA
004	Vennte (b) (7)(E) SEE SPEC SHEET	(b) (7)(E)	EA

Buy Attachment(s)

No.	Document Name	Document Size
001	(b) (7)(E)	172 KB
002		13 KB
003		215 KB

Bidding Requirements

Seller Attachment(s): In addition to providing pricing through the marketplace, Sellers MUST include certain non-pricing information as document(s) attached to their Bid, so they are received no later than the closing date and time of this Buy. Pricing will not be accepted if it is included in the attachment(s). Attachment(s) can total no more than 20 MB, whether multiple files or one file, and may be zipped to decrease their size. A Seller's failure to comply with these terms may result in its Bid being determined to be non-responsive. The attachment(s) must include the following non-pricing information: Please attach and spec sheet.

DHS FirstSource II Bids Only: Seller shall ONLY bid on this opportunity if they are able to provide commercially-available IT commodities, solutions, and value-added reseller (VAR) services per the requirements established in the Delivery Order solicitation. Seller shall adhere to all terms and conditions stated in their respective DHS FirstSource II IDIQ contract, AS WELL AS any additionally imposed through the Delivery Order solicitation - provided they do not contradict those executed by the former. Both the status of the Seller (i.e. its ability to conduct business with the Federal Government) and the status of the Seller's IDIQ contract shall be in an ACTIVE state at the time a bid is submitted.

Brand Name Only: The Buyer requests that Sellers bid only the Brand Name and part number provided (exact make, model, part number and/or description). This means that bids containing substitutions will be viewed as UNACCEPTABLE. If you are not able to deliver the line item as requested, DO NOT BID. Please direct any questions to the Buyer through our 'Submit a Question' button.

Minimum Bid Decrement is $100: The Buyer is requiring that any rebid must be lower than the 'current bid price' by this amount. The reduction is based on the total order and must be satisfied within the rebid minimum.

Purchase Order or Delivery Order: Buyer intends to issue award using a purchase order or delivery order. Bids from Sellers unable to accept purchase orders or delivery orders will not be considered for award.

Set-Aside Requirement: This solicitation is a HUBZone Small Business set-aside and only qualified Sellers can bid.

Use of Unison Marketplace: Buyers and Sellers agree to conduct this transaction through Unison Marketplace in compliance with the Unison Marketplace Terms of Use. Failure to comply with the below terms and conditions may result in offer being determined as non-responsive.

Evaluation Criteria/Basis of Award: Sellers understand that the Marketplace ranks all Bids by price; however, pursuant to applicable acquisition regulations and/or departmental guidelines, Buyers may use criteria other than price to evaluate offers. Accordingly, please note that, unless otherwise specified in the Buy Terms, below, to the extent required by applicable regulations and/or guidelines, award will be made to the responsible Seller whose offer conforming to the solicitation will be most advantageous to the Buyer on the basis of price, technical capability, delivery, and past performance.

Question Submission: Interested offerors must submit any questions concerning the solicitation at the earliest time possible to enable the buyer to respond. Questions can be submitted by using the 'Questions & Responses' link. Questions not received within a reasonable time prior to close of the solicitation may not be considered.

© 2019 Unison Marketplace Inc., All rights reserved.

Bidding Requirements

Default Terms: Unless otherwise specified in the Buy Terms, below, Bid must be good for 30 calendar days after close of Buy and shipping must be free on board (FOB) destination CONUS (Continental U.S.)

Buy Terms

Name	Criteria
Pricing Instructions	Unless the Buyer indicates otherwise within a particular line item description, each Seller shall include in its online Bid individual pricing for all required line items in order to be considered for award (i.e., Do not use the Included in another line item function when pricing each line item). If a line item cannot be separately priced, you must notify the buyer through the FedBid Submit a Question feature regarding which line item(s) should be included in which other line item(s) and request reposting. Failure to comply with this term may result in the Bid being determined to be non-responsive.
Equipment Condition	New Equipment ONLY; NO remanufactured or "gray market" items. All items must be covered by the manufacturer's warranty.
Offer Period	Bid MUST be good for 30 calendar days after close of Buy.
Shipping Condition	Shipping must be free on board (FOB) destination CONUS (Continental U.S.), which means that the seller must deliver the goods on its conveyance at the destination specified by the buyer, and the seller is responsible for the cost of shipping and risk of loss prior to actual delivery at the specified destination.
SAM Requirement	This solicitation requires registration with the System for Award Management (SAM) at the time an offer or quotation is submitted, excluding the exceptions outlined in FAR 4.1102(a). Registration information can be found at www.sam.gov.
ORCA Requirement	ORCA Requirement - Company must be registered on Online Representations and Certifications Application (ORCA) before an award could be made to them. If company is not registered with ORCA, they may do so by going to ORCA web site at https://orca.bpn.gov/.
Delivery Requirement	No partial shipments are permitted unless specifically authorized at the time of award.
Delivery Of Order	Delivery must be made within 30 days or less after receipt of order (ARO). The offeror must provide within its offer the number of days - not to exceed 30 - required to make delivery after it receives a purchase order from the buyer. Unless otherwise noted.
Q&A Instructions	Q&A -Please submit all questions by using the 'Submit a Question' button. This buy will then be reposted with Q&A based on the questions that come in (if applicable).
Award Criteria	Award Criteria-An award will be made to a responsive offeror (who submits all required submissions on time), whose past performance does not pose a risk to the Government, and whose offer is the Lowest Price Technically Acceptable (LPTA). An offer is technically acceptable if its technical capabilities conform to the Government's Statement of Work or listed specs whichever is applicable to the buy.
Supplemental Bid Information	Supplemental Bid Information In addition to providing pricing at www.FedBid.com for this solicitation, each Offeror must provide any required, NON-PRICING responses (e.g. technical proposal, representations and certifications, etc.) so that they are received no later than the closing date and time for this solicitation. Submissions can be sent to clientservices@fedbid.com.
For Exact Match Only Commodity Buys	For Exact Match Only Commodity Buys- NO SUBSTITUTIONS, EXACT MATCH ONLY. The vendor may not substitute any item/service listed on this order without prior written approval from the DHS/CBP Contracting Officer. No other individual is authorized, either verbally or in writing to change part numbers, manufacturer, quantity, delivery dates, or any other specifications of this RFQ. Items/services that do not conform to descriptions and part numbers found in this RFQ will be rejected at the time of delivery causing a return at the vendor's expense.
For Exact Match Services Buys Only	For Exact Match Services Buys Only- In order for a sellers bid to be 'responsive' and considered for award, the seller is REQUIRED to document exactly how they intend to meet the requirements of the SOW. They shall document statement detailing the service for evaluation. Failure to do this may be cause for termination. This information is REQUIRED in order for a sellers bid to be deemed 'responsive' and to be considered for award.
IPP Clause	In accordance with the IPP clause; ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016), payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: https:// www.ipp.gov. Contractor assistance with IPP enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866)

© 2019 Unison Marketplace Inc., All rights reserved.

Buy Terms

Name	Criteria
	973-3131. If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

Bid Summary

Seller	Bid #	Delivery Days	Total Price	Activity Notes
PANAMERICA COMPUTERS, INC. [DUNS: 166669742]	566657146	30	$1,068,317.18	0

© 2019 Unison Marketplace Inc., All rights reserved.

Competition Summary

(b) (5)

© 2019 Unison Marketplace Inc., All rights reserved.

Bid Details

PANAMERICA COMPUTERS, INC. [DUNS: 166669742] | Bid #566657146

Company Information

Bid Description:	[redacted] (b)(7)(E) & Venntel Software
Company Name:	PANAMERICA COMPUTERS, INC. [DUNS: 166669742]
Address:	1386 BIG OAK RD
City:	LURAY
State:	VA
Zip Code:	22835
Phone:	TBD
Fax:	
Duns No:	166669742
Cage Code:	301Q5
Tax ID:	541689773
Buy No:	984602
Socio-Economic Classification:	Small Business , Women-Owned Business , 8(A) , Minority-Owned Business , HUBZone Small Business , Small Disadvantaged Business , Women-Owned Small Business , Economically Disadvantaged Women-Owned Small Business

Seller Information

Sales Rep Name:	[redacted] (b) (6)
Address:	1386 Big Oak Rd
City:	Luray
State:	VA
Zip Code:	22835
Phone:	[redacted] (b) (6)
Fax:	
Email:	[redacted] (b) (6) @pcitec.com

CPARS Contractor Rep

Name:	[redacted] (b) (6)
Phone Number:	
Email:	[redacted] (b) (6) @pcitec.com

SAM Information

This information was obtained from the System for Award Management (SAM.gov) on 08/16/2019. Any due diligence required by any applicable parties, statutes or regulations should be used in accordance with FAR Subpart 42.15.

SAM Name:	PANAMERICA COMPUTERS, INC.
SAM DUNS:	166669742
Active Exclusion:	No
Registration Status:	Active
Expiration Date:	05/22/2020
Active Exclusion:	No

✓ **The vendor complies with all terms listed by the Buyer.**

Contract

⚠ **Notice:** This is a contract Buy. Before accepting, please verify that Line Item pricing does not exceed applicable contract pricing.

Contract No.:	HSHQDC-12-D-00013
Contract Owner:	PCi Tec
Contract Expiration Date:	09/16/2019
Delivery Days:	30

© 2019 Unison Marketplace Inc., All rights reserved.

Seller Attachment(s)

No.	Document Name	Document Size
001	(b)(7)(E)	648 KB
002		753 KB

Line Item(s)

Notice: This is a contract Buy. Before accepting, please verify that Line Item pricing does not exceed applicable contract pricing.

Item No.	Description	Qty	Unit Price	Ext. Price
001	Requested Specificatio (b) (7)(E) SEE SPEC SHEET Seller Line Item Details: **Descriptio** (b) (7)(E) SEE SPEC SHEET	(b) (7)(E	(b) (7)(E), (b) (4)	
002	Requested Specificatio (b) (7)(E) SEE SPEC SHEET Seller Line Item Details: **Descriptio** (b) (7)(E) SEE SPEC SHEET	(b) (7)(E		
003	Requested Specification: Venntel: Mobile device's Ad-tech ID data SEE SPEC SHEET Seller Line Item Details: **Description:** Venntel: Mobile device's Ad-tech ID data SEE SPEC SHEET	(b) (7)		
004	Requested Specification: Vennte (b) (7)(E) SEE SPEC SHEET Seller Line Item Details: **Description** (b) (7)(E) (b) (7)(E) SEE SPEC SHEET	(b) (7)		

Price Summary

Total Price: $1,068,317.18

ActivityCard® Information

Seller Summary

Seller	Member Since	Total Awards	Total Award Value	Notes
PANAMERICA COMPUTERS, INC. [DUNS: 166669742]	May-07	916	$ 168,065,337.18	0

© 2019 Unison Marketplace Inc., All rights reserved.

Buyer Activity

Buyer Organization	Bidding Since	Total Awards	Total Award Value
Bureau of Alcohol, Tobacco & Firearms	Feb-08	2	$ 20,006.00
Bureau of Indian Affairs	Jun-11	11	$ 425,290.23
Bureau of Public Debt	Aug-07	3	$ 63,039.07
Bureau of Reclamation	Aug-11	2	$ 9,068.31
C4IT Service Center TISCOM (Procurement)	Aug-14	3	$ 84,305.60
C4IT Service Center TISCOM (Purchase Card)	May-14	5	$ 925,349.07
Centers for Disease Control & Prevention	Jul-09	1	$ 12,003.59
DHHS FDA Office of Acquisitions and Grants Services	Jan-08	2	$ 27,355.24
DHHS IHS Indian Health Service	May-17	1	$ 1,220,110.24
DHHS NIH National Institute of Health	Feb-09	2	$ 137,579.96
DHS Citizenship and Immigration Services (CIS)	Dec-10	41	$ 13,870,654.25
DHS Customs and Border Protection	Oct-12	26	$ 123,373.83
DHS Customs and Border Protection (CBP)	Sep-07	375	$ 109,330,470.52
DHS Federal Emergency Management Agency	Jan-08	57	$ 2,880,220.96
DHS Federal Law Enforcement Training Center (FLETC)	Nov-12	20	$ 1,237,841.11
DHS Immigration and Customs Enforcement (ICE)	Aug-08	63	$ 5,157,394.70
DHS Office of Procurement Operations (OPO)	Jul-11	61	$ 16,943,030.70
DHS Transportation Security Administration (TSA)	Jul-08	20	$ 5,823,604.80
DHS United States Coast Guard Headquarters	Jun-13	1	$ 61,695.70
DHS United States Secret Service	Jul-14	2	$ 31,851.29
DOC NOAA AGO Strategic Sourcing Acquisition Division	Aug-12	1	$ 30,167.34
DOC NOAALink	Aug-12	7	$ 551,596.12
DOC National Institute of Standards and Technology	Sep-07	1	$ 12,987.18
DOC Office of the Secretary	Aug-12	1	$ 136,114.90
DOI BIA - Western Region	Aug-11	4	$ 76,637.63
DOI BLM Arizona Region	Aug-11	1	$ 1,708.73
DOI BLM Eastern States/ Headquarters	Aug-11	1	$ 139,803.62
DOI BLM Idaho Region	Aug-11	1	$ 25,208.64

© 2019 Unison Marketplace Inc., All rights reserved.

Buyer Activity

Buyer Organization	Bidding Since	Total Awards	Total Award Value
DOI BLM Montana Region	Jun-11	1	$ 6,062.58
DOI Fish & Wildlife Service	May-11	30	$ 397,487.06
DOI NPS Alaska Region - National Park Service	Aug-15	1	$ 9,515.20
DOI NPS Denver Service Center - National Park Service	Sep-11	1	$ 10,403.00
DOI NPS Intermountain Northern Rockies Buying Office	Dec-13	1	$ 4,013.68
DOI NPS Northeast Region - National Park Service	Aug-11	1	$ 69,901.34
DOI NPS Northeast Virginia Buying Office	Jul-15	1	$ 5,999.99
DOI NPS Pacific West Golden Gate Buying Office	Jul-15	1	$ 20,018.55
DOI NPS Pacific West Olympic National Park Buying Office	Sep-13	1	$ 1,810.71
DOI NPS Pacific West SF/ SEA Buying Office	Jul-13	1	$ 8,363.38
DOI NPS WCP - Washington Contracting Procurement Office	Sep-11	2	$ 16,045.99
DOL BLS Washington DC	Jun-13	8	$ 261,116.32
DOL Office of Procurement Services	Dec-13	5	$ 664,381.77
DOS Embassy/Bogota, Colombia NAS- Department of State	Oct-07	1	$ 2,161.97
DOS Embassy/Others	Jul-07	1	$ 4,908.80
DOS Office of Inspector General - Department of State	Dec-15	1	$ 13,696.00
Department of Interior	Aug-12	4	$ 276,842.73
Department of State	Jul-07	28	$ 3,309,721.13
EPA - OFFICE OF ACQUISITION MANAGEMENT (OAM)	Aug-07	7	$ 225,111.71
FLC - Jacksonville	Dec-12	4	$ 43,956.15
FLC - Norfolk	Aug-11	3	$ 213,961.11
FLC Norfolk - Philadelphia	Jan-14	1	$ 31,902.50
Federal Bureau of Investigation	Feb-08	5	$ 270,585.54
INSCOM - Fort Belvoir	May-13	1	$ 92,277.52
MICC Fort AP Hill	Aug-13	1	$ 7,180.12
MICC Fort Drum	Jul-09	1	$ 25,478.46
MICC Fort Eustis	Nov-08	1	$ 124,573.32
MICC Fort Gordon	Aug-08	2	$ 50,701.21
MICC Fort Irwin	Aug-08	1	$ 8,489.26

© 2019 Unison Marketplace Inc., All rights reserved.

Buyer Activity

Buyer Organization	Bidding Since	Total Awards	Total Award Value
MICC Joint Base San Antonio	Feb-08	1	$ 5,141.55
NAVSEA NSWC - Dahlgren	Jul-13	1	$ 90,143.66
NAVSEA SUPSHIP - Newport News	Feb-08	3	$ 53,058.24
NCR - Alexandria	Sep-08	1	$ 17,784.84
NPS Southeast North Buying Office	Jul-15	1	$ 6,716.42
NSWC Carderock - Philadelphia	Jun-13	6	$ 86,620.93
NSWC Port Hueneme	Aug-13	1	$ 8,879.94
National Oceanic & Atmospheric Administration	Jul-08	2	$ 18,150.26
National Park Service	Jun-11	40	$ 522,813.74
National Science Foundation	Feb-09	2	$ 475,303.41
Strategic Systems Programs	Mar-10	1	$ 18,529.36
U.S. Embassy Warsaw, Poland	Aug-13	1	$ 4,760.66
US Geological Survey	Jun-11	19	$ 296,931.94
United States International Trade Commission	Aug-12	2	$ 99,590.64
VHA NCO 04 - 642 - Philadelphia, PA	Sep-12	1	$ 7,433.16
VHA NCO 07 - 557 - Dublin, GA	Jun-12	1	$ 4,299.22
VHA NCO 12 - 69D - GLAC - Milwaukee, WI	Sep-11	1	$ 4,043.78
Virginia Contracting Activity	Jun-16	1	$ 809,999.00

Seller Activity Notes History *(within 18 months)*

Note: The Seller Activity Note IS NOT A PERFORMANCE EVALUATION per FAR Subpart 42.15, and it is not intended to be used as such. Buyers are encouraged to conduct due diligence and past performance reviews as required by any applicable policies, statutes or regulations.

Buy #	Solicitation #	Bid #	Create Date	Buyer Organization	Note Created By
There is no note activity to display					

Chronology

Buy #	Status	Status Date/ Time	Solicitation #	Contract Type	Set Aside	Start Date/Time	End Date/Time
984602	Pending Award	08/15/2019 17:00	20111511	DHS FirstSource II	HUBZone Small Business	08/08/2019 15:23	08/15/2019 17:00

© 2019 Unison Marketplace Inc., All rights reserved.

My Comments

Buy #	Initiator	Timestamp	Note

No comments found.

Current Questions / Responses

Buy # 984602 **Seller Question Deadline: No Seller Question Deadline Set**

Quest. #	Timestamp	Description	Asked By	Seller Organization
593396	08/15/2019 14:25	EXTENSION REQUEST FROM A SELLER: Please provide an extension for this bid, we are still working on pricing, thank you. !	(b) (6) [redacted]	C & C INTERNATIONAL COMPUTERS & CONSULTANTS, INC. [DUNS: 932469612]
	08/15/2019 15:04	**BUYER RESPONSE** The Buy is being extended		

© 2019 Unison Marketplace Inc., All rights reserved.

Reverse Auction Results for: 946089

Report generated 09/10/2018 10:19:43 ET

Buy Information

Buyer Organization: DHS Customs and Border Protection (CBP)
Buyer Re [redacted] (b)(6) (b)(7)(C)
Buy Description: Infrastructure Equipment for Tri Cities Global Enrollment Center
Internal Description: Infrastructure Equipment for Tri Cities Global Enrollment Center
Solicitation No.: 20107297
Start Date / Time: 08/30/2018 08:19 ET
End Date / Time: 09/05/2018 18:00 ET

Set-Aside Requirement: HUBZone Small Business
Contract Vehicle: DHS FirstSource II
Seller Community: DHS FirstSource II – HUBZone Socioeconomic Category

FedBizOpps Solicitation: No
FAC: 2005-100
Purchase Description: Brand Name or Equal
Specialized Buy Type: No
Award Type: Purchase Order or Delivery Order
Seller Attachments: Attachments Optional
Seller Question Deadline: No Seller Question Deadline Set - None
Final Bid: No

Your Bid Summary

Total Sellers Notified: 6
Total Sellers Bidding: 1
Number of Bids: 2
Number of No Bids: 2

Target Price

Total Target Price: $772,500.00 - Target Price is Active
Bid Decrement: $100

Suggested Sellers

Company Name	Phone	Sales Rep	Email
No sellers added			

Category

PSC 70 -- Information Technology (ADP) Equipment (Including Firmware), Software, Supplies and Support Equipment

Sub-category

PSC 7050 -- IT Components

NAICS

541690 -- Other Scientific and Technical Consulting Services

© 2001 - 2018 FedBid, Inc. All rights reserved.

Delivery	Shipping Address
30 Day(s) - **Required** (No. of calendar days after receipt of order (ARO) by which Buyer requires Seller to deliver)	See Statement of Work

Line Item(s)

Item No.	Description	Qty	Unit
001	(SEE SOW FOR DETAILS)	(b) (7)(E) [redacted]	EA
002	(SEE SOW FOR DETAILS)		EA
003	(SEE SOW FOR DETAILS)		EA
004	(SEE SOW FOR DETAILS)		EA

Buy Attachment(s)

No.	Document Name	Document Size
001	(b) (7)(E)	180 KB
002		16 KB

Bidding Requirements

Seller Attachment(s): In addition to providing pricing through the marketplace, Sellers have the OPTION to include certain non-pricing information as document(s) attached to their Bid, so they are received no later than the closing date and time of this Buy. Pricing will not be accepted if it is included in the attachment(s). Attachment(s) can total no more than 20 MB, whether multiple files or one file, and may be zipped to decrease their size. A Seller's failure to comply with these terms may result in its Bid being determined to be non-responsive. The attachment(s) should include the following non-pricing information: Please attach additional specification for technical evaluation.

DHS FirstSource II Bids Only: Seller shall ONLY bid on this opportunity if they are able to provide commercially-available IT commodities, solutions, and value-added reseller (VAR) services per the requirements established in the Delivery Order solicitation. Seller shall adhere to all terms and conditions stated in their respective DHS FirstSource II IDIQ contract, AS WELL AS any additionally imposed through the Delivery Order solicitation - provided they do not contradict those executed by the former. Both the status of the Seller (i.e. its ability to conduct business with the Federal Government) and the status of the Seller’s IDIQ contract shall be in an ACTIVE state at the time a bid is submitted.

Brand Name or Equal: The Buyer is allowing Sellers to submit bids for alternate items, provided those items meet all of the salient physical, functional, or performance characteristics specified by this solicitation. Sellers MUST enter exactly what they are bidding (including make, model and description) into the blank description field in order for the bid to be considered. The Buyer will evaluate 'equal' items on the basis of information furnished by the Seller or identified in the bid and reasonably available to the Buyer. The Buyer is not responsible for locating or obtaining any information not identified in the Bid.

Minimum Bid Decrement is $100: The Buyer is requiring that any rebid must be lower than the 'current bid price' by this amount. The reduction is based on the total order and must be satisfied within the rebid minimum.

Purchase Order or Delivery Order: Buyer intends to issue award using a purchase order or delivery order. Bids from Sellers unable to accept purchase orders or delivery orders will not be considered for award.

Set-Aside Requirement: This solicitation is a HUBZone Small Business set-aside and only qualified Sellers can bid.

Use of FedBid: Buyers and Sellers agree to conduct this transaction through FedBid in compliance with the FedBid Terms of Use. Failure to comply with the below terms and conditions may result in offer being determined as non-responsive.

© 2001 - 2018 FedBid, Inc. All rights reserved.

Bidding Requirements

Evaluation Criteria/Basis of Award: Sellers understand that the Marketplace ranks all Bids by price; however, pursuant to applicable acquisition regulations and/or departmental guidelines, Buyers may use criteria other than price to evaluate offers. Accordingly, please note that, unless otherwise specified in the Buy Terms, below, to the extent required by applicable regulations and/or guidelines, award will be made to the responsible Seller whose offer conforming to the solicitation will be most advantageous to the Buyer on the basis of price, technical capability, delivery, and past performance.

Question Submission: Interested offerors must submit any questions concerning the solicitation at the earliest time possible to enable the buyer to respond. Questions can be submitted by using the 'Questions & Responses' link. Questions not received within a reasonable time prior to close of the solicitation may not be considered.

Default Terms: Unless otherwise specified in the Buy Terms, below, Bid must be good for 30 calendar days after close of Buy and shipping must be free on board (FOB) destination CONUS (Continental U.S.)

Buy Terms

Name	Criteria
Pricing Instructions	Unless the Buyer indicates otherwise within a particular line item description, each Seller shall include in its online Bid individual pricing for all required line items in order to be considered for award (i.e., Do not use the Included in another line item function when pricing each line item). If a line item cannot be separately priced, you must notify the buyer through the FedBid Submit a Question feature regarding which line item(s) should be included in which other line item(s) and request reposting. Failure to comply with this term may result in the Bid being determined to be non-responsive.
Equipment Condition	New Equipment ONLY; NO remanufactured or "gray market" items. All items must be covered by the manufacturer's warranty.
Offer Period	Bid MUST be good for 30 calendar days after close of Buy.
Shipping Condition	Shipping must be free on board (FOB) destination CONUS (Continental U.S.), which means that the seller must deliver the goods on its conveyance at the destination specified by the buyer, and the seller is responsible for the cost of shipping and risk of loss prior to actual delivery at the specified destination.
SAM Requirement	This solicitation requires registration with the System for Award Management (SAM) prior to award, pursuant to applicable regulations and guidelines. Registration information can be found at www.sam.gov.
ORCA Requirement	ORCA Requirement - Company must be registered on Online Representations and Certifications Application (ORCA) before an award could be made to them. If company is not registered with ORCA, they may do so by going to ORCA web site at https://orca.bpn.gov/.
Delivery Requirement	No partial shipments are permitted unless specifically authorized at the time of award.
Delivery Of Order	Delivery must be made within 30 days or less after receipt of order (ARO). The offeror must provide within its offer the number of days - not to exceed 30 - required to make delivery after it receives a purchase order from the buyer. Unless otherwise noted.
Q&A Instructions	Q&A -Please submit all questions by using the 'Submit a Question' button. This buy will then be reposted with Q&A based on the questions that come in (if applicable).
Award Criteria	Award Criteria-An award will be made to a responsive offeror (who submits all required submissions on time), whose past performance does not pose a risk to the Government, and whose offer is the Lowest Price Technically Acceptable (LPTA). An offer is technically acceptable if its technical capabilities conform to the Government's Statement of Work or listed specs whichever is applicable to the buy.
Supplemental Bid Information	Supplemental Bid Information In addition to providing pricing at www.FedBid.com for this solicitation, each Offeror must provide any required, NON-PRICING responses (e.g. technical proposal, representations and certifications, etc.) so that they are received no later than the closing date and time for this solicitation. Submissions can be sent to clientservices@fedbid.com.

© 2001 - 2018 FedBid, Inc. All rights reserved.

Buy Terms

Name	Criteria
For Exact Match Only Commodity Buys	For Exact Match Only Commodity Buys- NO SUBSTITUTIONS, EXACT MATCH ONLY. The vendor may not substitute any item/service listed on this order without prior written approval from the DHS/CBP Contracting Officer. No other individual is authorized, either verbally or in writing to change part numbers, manufacturer, quantity, delivery dates, or any other specifications of this RFQ. Items/services that do not conform to descriptions and part numbers found in this RFQ will be rejected at the time of delivery causing a return at the vendor's expense.
For Exact Match Services Buys Only	For Exact Match Services Buys Only- In order for a sellers bid to be 'responsive' and considered for award, the seller is REQUIRED to document exactly how they intend to meet the requirements of the SOW. They shall document statement detailing the service for evaluation. Failure to do this may be cause for termination. This information is REQUIRED in order for a sellers bid to be deemed 'responsive' and to be considered for award.
For Buys other than Exact Match:	For all buys other than Exact Match Sellers MUST document what they are bidding for evaluation for award. Sellers must include, extended specs and/or manufacturer name and part numbers (if applicable). Failure to do this may be cause for termination. This information is REQUIRED in order for a sellers bid to be deemed 'responsive' and to be considered for award. FAR 52.211-6
IPP Clause	In accordance with the IPP clause; ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016), payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: https:// www.ipp.gov. Contractor assistance with IPP enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131. If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

Bid Summary

Seller	Bid #	Delivery Days	Total Price	Activity Notes
	565063147	30		0

Bid Details

| **Bid #565063147**

Company Information

Bid Description: Misc Softwar [redacted] Venntel

Company Name:
Address:
City:
State:
Zip Code:
Phone:

Seller Information

Sales Rep Name:
Address:
City:
State:
Zip Code:
Phone:
Fax:
Email:

© 2001 - 2018 FedBid, Inc. All rights reserved.

Fax:	
Duns No:	
Cage Code:	
Tax ID:	
FedBid Buy No:	946089
Socio-Economic Classification:	Small Business , Women-Owned Business , 8(A) , Minority-Owned Business , HUBZone Small Business , Small Disadvantaged Business , Women-Owned Small Business , Economically Disadvantaged Women-Owned Small Business

CPARS Contractor Rep

Name:	
Phone Number:	
Email:	

✓ **The vendor complies with all terms listed by the Buyer.**

Contract

⚠ **Notice:** This is a contract Buy. Before accepting, please verify that Line Item pricing does not exceed applicable contract pricing.

Contract No.:	
Contract Owner:	
Contract Expiration Date:	09/16/2018
Delivery Days:	30

Seller Attachment(s)

No.	Document Name	Document Size
No Seller Attachment(s)		

Line Item(s)

⚠ **Notice:** This is a contract Buy. Before accepting, please verify that Line Item pricing does not exceed applicable contract pricing.

Item No.	Description	Qty	Unit Price	Ext. Price
001	Requested Specification: (SEE SOW FOR DETAILS) (b) (7)(E)	(b) (7)(E)		
002	Requested Specification: (SEE SOW FOR DETAILS) (b) (7)(E)			
003	Requested Specification: (SEE SOW FOR DETAILS)			

© 2001 - 2018 FedBid, Inc. All rights reserved.

Line Item(s)

Item No.	Description	Qty	Unit Price	Ext. Price
	(b) (7)(E)			
004	Requested Specification: (SEE SOW FOR DETAILS) Seller Line Item Details: **Manufacturer:** Venntel **Part Number:** Mobile device Ad-tech **Description:** Venntel: Mobile device's Ad-tech ID data	[redacted]		

Price Summary

Total Price:

ActivityCard® Information

Seller Summary

Seller	Member Since	Total Awards	Total Award Value	Notes
	May-07	842	$ 133,021,558.30	0

Buyer Activity

Buyer Organization	Bidding Since	Total Awards	Total Award Value
Bureau of Alcohol, Tobacco & Firearms	Feb-08	2	$ 20,006.00
Bureau of Indian Affairs	Jun-11	11	$ 425,290.23
Bureau of Public Debt	Aug-07	3	$ 63,039.07
Bureau of Reclamation	Aug-11	2	$ 9,068.31
C4IT Service Center TISCOM (Procurement)	Aug-14	3	$ 84,305.60
C4IT Service Center TISCOM (Purchase Card)	May-14	5	$ 925,349.07
Centers for Disease Control & Prevention	Jul-09	1	$ 12,003.59
DHHS FDA Office of Acquisitions and Grants Services	Jan-08	2	$ 27,355.24
DHHS IHS Indian Health Service	May-17	1	$ 1,220,110.24
DHHS NIH National Institute of Health	Feb-09	2	$ 137,579.96

© 2001 - 2018 FedBid, Inc. All rights reserved.

Buyer Activity

Buyer Organization	Bidding Since	Total Awards	Total Award Value
DHS Citizenship and Immigration Services (CIS)	Dec-10	41	$ 13,887,384.92
DHS Customs and Border Protection	Oct-12	22	$ 108,214.71
DHS Customs and Border Protection (CBP)	Sep-07	321	$ 77,995,702.04
DHS Federal Emergency Management Agency	Jan-08	54	$ 2,719,612.91
DHS Federal Law Enforcement Training Center (FLETC)	Nov-12	20	$ 1,237,841.11
DHS Immigration and Customs Enforcement (ICE)	Aug-08	57	$ 4,872,357.91
DHS Office of Procurement Operations (OPO)	Jul-11	61	$ 16,943,030.70
DHS Transportation Security Administration (TSA)	Jul-08	17	$ 5,330,275.24
DHS United States Coast Guard Headquarters	Jun-13	1	$ 61,695.70
DHS United States Secret Service	Jul-14	2	$ 31,851.29
DOC NOAA AGO Strategic Sourcing Acquisition Division	Aug-12	1	$ 30,167.34
DOC NOAALink	Aug-12	7	$ 551,596.12
DOC National Institute of Standards and Technology	Sep-07	1	$ 12,987.18
DOC Office of the Secretary	Aug-12	1	$ 136,114.90
DOI BIA - Western Region	Aug-11	4	$ 76,637.63
DOI BLM Arizona Region	Aug-11	1	$ 1,708.73
DOI BLM Eastern States/ Headquarters	Aug-11	1	$ 139,803.62
DOI BLM Idaho Region	Aug-11	1	$ 25,208.64
DOI BLM Montana Region	Jun-11	1	$ 6,062.58
DOI Fish & Wildlife Service	May-11	30	$ 397,487.06
DOI NPS Alaska Region - National Park Service	Aug-15	1	$ 9,515.20
DOI NPS Denver Service Center - National Park Service	Sep-11	1	$ 10,403.00
DOI NPS IMR NORTHERN ROCKIES MABO	Dec-13	1	$ 4,013.68
DOI NPS NER VA MABO	Jul-15	1	$ 5,999.99

© 2001 - 2018 FedBid, Inc. All rights reserved.

Buyer Activity

Buyer Organization	Bidding Since	Total Awards	Total Award Value
DOI NPS Northeast Region - National Park Service	Aug-11	1	$ 69,901.34
DOI NPS PWR GOGA MABO	Jul-15	1	$ 20,018.55
DOI NPS PWR OLYM MABO	Sep-13	1	$ 1,810.71
DOI NPS PWR SF/SEA MABO	Jul-13	1	$ 8,363.38
DOI NPS SER NORTH MABO	Jul-15	1	$ 6,716.42
DOI NPS WCP - Washington Contracting Procurement Office	Sep-11	2	$ 16,045.99
DOL BLS Washington DC	Jun-13	8	$ 261,116.32
DOL Office of Procurement Services	Dec-13	5	$ 664,381.77
DOS Embassy/Bogota, Colombia NAS-Department of State	Oct-07	1	$ 2,161.97
DOS Embassy/Others	Jul-07	1	$ 4,908.80
DOS Office of Inspector General - Department of State	Dec-15	1	$ 13,696.00
Department of Interior	Aug-12	3	$ 131,317.98
Department of State	Jul-07	26	$ 746,221.14
EPA - OFFICE OF ACQUISITION MANAGEMENT (OAM)	Aug-07	7	$ 225,111.71
FLC - Jacksonville	Dec-12	4	$ 43,956.15
FLC - Norfolk	Aug-11	2	$ 151,378.30
FLC Norfolk - Philadelphia	Jan-14	1	$ 31,902.50
Federal Bureau of Investigation	Feb-08	5	$ 270,585.54
INSCOM - Fort Belvoir	May-13	1	$ 92,277.52
MICC Fort AP Hill	Aug-13	1	$ 7,180.12
MICC Fort Drum	Jul-09	1	$ 25,478.46
MICC Fort Eustis	Nov-08	1	$ 124,573.32
MICC Fort Gordon	Aug-08	2	$ 50,701.21
MICC Fort Irwin	Aug-08	1	$ 8,489.26
MICC Joint Base San Antonio	Feb-08	1	$ 5,141.55
NAVSEA NSWC - Dahlgren	Jul-13	1	$ 90,143.66
NAVSEA SUPSHIP - Newport News	Feb-08	3	$ 53,058.24
NCR - Alexandria	Sep-08	1	$ 17,784.84
NSWC Carderock - Philadelphia	Jun-13	6	$ 86,620.93
NSWC Port Hueneme	Aug-13	1	$ 8,879.94

© 2001 - 2018 FedBid, Inc. All rights reserved.

Buyer Activity

Buyer Organization	Bidding Since	Total Awards	Total Award Value
National Oceanic & Atmospheric Administration	Jul-08	2	$ 18,150.26
National Park Service	Jun-11	40	$ 522,813.74
National Science Foundation	Feb-09	2	$ 475,303.41
Strategic Systems Programs	Mar-10	1	$ 18,529.36
U.S. Embassy Warsaw, Poland	Aug-13	1	$ 4,760.66
US Geological Survey	Jun-11	19	$ 296,931.94
United States International Trade Commission	Aug-12	2	$ 99,590.64
VHA NCO 04 - 642 - Philadelphia, PA	Sep-12	1	$ 7,433.16
VHA NCO 07 - 557 - Dublin, GA	Jun-12	1	$ 4,299.22
VHA NCO 12 - 69D - GLAC - Milwaukee, WI	Sep-11	1	$ 4,043.78
Virginia Contracting Activity	Jun-16	1	$ 809,999.00

Seller Activity Notes History *(within 18 months)*

Note: The Seller Activity Note IS NOT A PERFORMANCE EVALUATION per FAR Subpart 42.15, and it is not intended to be used as such. Buyers are encouraged to conduct due diligence and past performance reviews as required by any applicable policies, statutes or regulations.

Buy #	Solicitation #	Bid #	Create Date	Buyer Organization	Note Created By
There is no note activity to display					

Chronology

Buy #	Status	Status Date/Time	Solicitation #	Contract Type	Set Aside	Start Date/Time	End Date/Time
946089	Pending Award	09/05/2018 18:00	20107297	DHS FirstSource II	HUBZone Small Business	08/30/2018 08:19	09/05/2018 18:00

My Comments

Buy #	Initiator	Timestamp	Note
No comments found.			

© 2001 - 2018 FedBid, Inc. All rights reserved.

Current Questions / Responses

Buy # 946089 Seller Question Deadline: No Seller Question Deadline Set

Quest. #	Timestamp	Description	Asked By	Seller Organization
562051	09/05/2018 16:55	FEEDBACK FROM A SELLER: Please thank the CO for the extension, but the salesrep at Venntel who said over the phone he would quote, later sent an email and refused to quote: "I received the SOW that was sent over. I've already provided quotes to an authorized reseller for this opportunity. (b) (6) at C & C INTERNATIONAL COMPUTERS & CONSULTANTS, INC. [DUNS: 932469612] **BUYER RESPONSE** No Response	FedBid	FedBid
561966	09/05/2018 14:21	EXTENSION REQUEST FROM A SELLER: Can you please request an extension? I've been promised quotes on the remaining 2 items but have yet to receive them (b) (6) (b) (6) at C & C INTERNATIONAL COMPUTERS & CONSULTANTS, INC. [DUNS: 932469612]	FedBid	FedBid
	09/05/2018 14:28	**BUYER RESPONSE** 'No Reply'		
561136	08/30/2018 15:26	REQUEST FROM A SELLER: Good afternoon. Can you please provide a point of contact f (b)(7)(E) Thanks!	(b) (6)	PANAMERICA COMPUTERS, INC. [DUNS: 166669742]
	09/05/2018 10:02	**RELEASED TO ALL SELLERS** **REVISED SELLER QUESTION** Can you please provide a point of contact f (b)(7)(E) ? Thanks! **BUYER RESPONSE** (b) (6), (b) (7)(E)		

© 2001 - 2018 FedBid, Inc. All rights reserved.

SDRD5204

Office of Information and Technology

Service Delivery Requirement Document

CBP Originating Office: Office of Field Operations

Originating Office Point of Contact (POC) Troy Miller

Originating Office POC phone number:

Date of request: 05/06/15

Detailed description of requirement: Requirements in support of counter network operations for OFO National Targeting Center .

Historical information/Background on requirement: (i.e. response to trouble ticket, user issues etc. or is an OIT recommended action):

Through a fiscal year 2015 direct appropriation, Customs and Border Protection (CBP)/National Targeting Center (NTC) received a (b) (7)(E) allocation for Counter Network Operations. The specific language in the appropriation identified three elements:

1. Focused analytics effort for data science and intelligence analysis;
2. Advanced (b) (7)(E) to better understand and define (b) (7)(E) (b) (7)(E)
3. Hardware and (b) (7)(E) (b) (7)(E)

Funding source

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

	Current FY 2015	FY+1 2016	FY+2 2017	FY+3 2018	FY+4 2019	FY+5 2020
(b) (7)(E)						

(b) (7)(E)

Detailed description of Government Position: (include number of FTE, grade, and description of work to be performed): N/A

Detailed description of new investment cost (for each FY as applicable): In an effort to enhance Targeting and Counter Network Operations, it is necessary to have a (b) (7)(E)

(b) (7)(E)

Focused analytics effort for data science and intelligence analysis.

- Additional contractor support to (b) (7)(E) and other information to (b) (7)(E)
- Increase collaboration with (b) (7)(E) (b) (7)(E).

1. Advanced a(b) (7)(E) to better understand and (b) (7)(E)
   - Acquisition of(b) (7)(E) (b) (7)(E).

2. Hardware and(b) (7)(E) to enable collaborative(b) (7)(E) (b) (7)(E).
   - Infrastructure support to existing (b) (7)(E) (b) (7)(E).

Detailed description of Operations and Maintenance cost (for each year as applicable): Currently the outyear(b) (7)(E)

(b) (7)(E)

Approved by Originating Office : Name (b) (6), (b) (7)(C) Date

Signature of approval from Originating office : (b) (6), (b) (7)(C) Date 11/12/2015

Approved by Originating Office HQ Budget Officer: Name (b) (6), (b) (7)(C) Date 5/12/15

Signature of approval from originating office HQ Budget Officer (b) (6), (b) (7)(C)

To be used by OIT below the dotted line

Confirmation that EDME, FS and ENTS have been consulted and that there costs are included (indicate below of consulted and if costs are included):

EDME_____ ENTS_____ FS_____

SDRD6395

Office of Information and Technology

Service Delivery Requirement Document

CBP Originating Office: OFO

Originating Office Point of Contact (POC) (name): (b) (6), (b) (7)(C)

Originating Office POC phone number: (b) (6), (b) (7)(C)

Date of request: August 22, 2016

Detailed description of requirement:

OIT support of OFO-NTC Counter Network Division (b) (7)(E):

A. Contract OSINT Analyst Support Staff - (b) (7)(E)
   - Provide direct OSINT research support and analysis for (b) (7)(E) (b) (7)(E)
     - OSINT research will allow (b) (7)(E) (b) (7)(E) and identify Open Source DEROG and positive confirmatory information pertaining to (b) (7)(E) (b) (7)(E)
   - Contract support will provide staffing and manpower to advance the initial goals and stand-up of the CBP (b) (7)(E) c(b) (7)(E)s tasked with providing enterprise-wide open source and social media research assistance and best practices, develop training programs, liaising with external partners, and supporting strategic, operational, and tactical priorities through the use of open source and social media research and analysis for all of CBP

B. Administrative Costs - (b) (7)(E)
   - Administrative costs will provide for contractor travel costs and support costs associated with the deployment of standardized OSINT training programs across the CBP enterprise
   - Administrative costs will also cover miscellaneous contractor costs and case-by-case deployment of advanced industry technologies and analytics programs.

Historical information/Background on requirement: (i.e. response to trouble ticket, user issues etc. or is an OIT recommended action): N/A

Funding source

The Office of Field Operations agrees to provide the current year costs identified below. This is a one-time transfer and does not have out-year costs.

	Current FY 2016	FY+1 2017	FY+2 2018	FY+3 2019	FY+4 2020	FY+5 2021
(b) (7)(E)						

Detailed description of travel: N/A

Detailed description of new investment cost (for each FY as applicable):

OIT support of OFO-NTC Counter Network Division (b) (7)(E) :

A. **Contract OSINT Analyst Support Staff –** (b) (7)(E)
   - **Provide direct OSINT research support and analysis for** (b) (7)(E) (b) (7)(E)
     - **OSINT research will allow** (b) (7)(E) (b) (7)(E) **and identify Open Source DEROG and positive, confirmatory information pertaining to** (b) (7)(E) (b) (7)(E)
   - **Contract support will provide staffing and manpower to advance the initial goals and stand-up of the CBP** (b) (7)(E)
     - (b) (7)(E) **is tasked with providing enterprise-wide open source and social media research assistance and best practices, develop training programs, liaising with external partners, and supporting strategic, operational, and tactical priorities through the use of open source and social media research and analysis for all of CBP**

B. **Administrative Costs -** (b) (7)(E)
   - **Administrative costs will provide for contractor travel costs and support costs associated with the deployment of standardized OSINT training programs across the CBP enterprise**
   - **Administrative costs will also cover miscellaneous contractor costs and case-by-case deployment of advanced industry technologies and analytics programs.**

Detailed description of Operations and Maintenance cost (for each FY as applicable): N/A

Approved by Originating Office: (b) (6), (b) (7)(C) Date 8/22/16

Signature of approval from Originating o (b) (6), (b) (7)(C) Date 8/22/16

Approved by Originating Office HQ Budget Officer: Name (b) (6), (b) (7)(C) Date 8/22/16

Signature of approval from originating office HQ Budget Officer (b) (6), (b) (7)(C)

To be used by OIT below the dotted line

Confirmation that EDME, FS and ENTS have been consulted and that there costs are included (indicate below of consulted and if costs are included):

EDME_____ **ENTS**_____ **FS**_____

Invoice

PCiTeC™ PANAMERICA COMPUTERS, INC.
1386 BIG OAK ROAD, LURAY, VA 22835
Tel: 540 635 4402 Fax: 540 635 8871

DUNS# 166669742
TAX ID# 54-1689773

Invoice #	208696
Invoice Date	9/30/2019
Cust. ID No.	208696

Bill To
DHS/CBP
WWW.IPP
[redacted] (b)(6) (b)(7)(C) @cbp.dhs.gov
cbp.dhs.gov

Ship To
DHS/CBP
ATTN [redacted] (b)(6) (b)(7)(C)
PO: 70B04C19F00000802
5971 KINGSTOWNE VILLAGE PKWY., 5TH FLR MR
ALEXANDRIA, VA 22315

P.O. Number	Order Date	Terms	Sales Rep	Via	F.O.B.
70B04C19F00000802	9/24/2019	Net 30	[redacted] (b) (6)	DROP SHIP	Destination

Line Ite...	Part #	Description	Quantity	Unit Price	Amount
	ACCEL PMT	Panamerica Computers, Inc. is a HUBZone, small disadvantaged, woman owned business and therefore qualifies for accelerated payment in accordance with OMB MEMO M 11 32.			
	FSII HUBZONE	FIRST SOURCE II HSHQDC 12 D 00013 ORDER # 70B04C19F00000802 REQ # 0020111511 Reference Bid # 566657146, dated 8/15/2019, from Unison Buy # 984602 Period of Performance: 9/27/2019 9/25/2020			

SEE REVERSE FOR ADDITIONAL TERMS AND CONDITIONS.

[redacted] (b) (4)

Subtotal	
Sales Tax (5.3%)	
Total	
Payments/Credits	
Balance Due	

A HUBZone, WOSB and SWaM CERTIFIED COMPANY
IF YOU HAVE QUESTIONS REGARDING THIS INVOICE PLEASE CONTAC [redacted] (b) (6)
[redacted] (b) (6)

Invoice

PCiTeC™ PANAMERICA COMPUTERS, INC.
1386 BIG OAK ROAD, LURAY, VA 22835
Tel: 540 635 4402 Fax: 540 635 8871

DUNS# 166669742
TAX ID# 54-1689773

Invoice #	208696
Invoice Date	9/30/2019
Cust. ID No.	(b) (4)

Bill To
DHS/CBP
WWW.IPP
(b)(6) (b)(7)(C) @cbp.dhs.gov
@cbp.dhs.gov

Ship To
DHS/CBP
ATTN (b)(6) (b)(7)(C)
PO: 70B04C19F00000802
5971 KINGSTOWNE VILLAGE PKWY., 5TH FLR MR
ALEXANDRIA, VA 22315

P.O. Number	Order Date	Terms	Sales Rep	Via	F.O.B.
70B04C19F00000802	9/24/2019	Net 30	(b) (6)	DROP SHIP	Destination

Line Ite...	Part #	Description	Quantity	Unit Price	Amount
10	(b) (7)	(b) (7)(E)		(b) (7)(E), (b) (4)	
20	(b) (7)(E)				

SEE REVERSE FOR ADDITIONAL TERMS AND CONDITIONS.
(b) (4)

Subtotal	
Sales Tax (5.3%)	
Total	
Payments/Credits	
Balance Due	

A HUBZone, WOSB and SWaM CERTIFIED COMPANY
IF YOU HAVE QUESTIONS REGARDING THIS INVOICE PLEASE CONTAC (b) (6) (b) (6)

Invoice

PCiTeC™ PANAMERICA COMPUTERS, INC.
1386 BIG OAK ROAD, LURAY, VA 22835
Tel: 540 635 4402 Fax: 540 635 8871

DUNS# 166669742
TAX ID# 54-1689773

Invoice # 208696
Invoice Date 9/30/2019
Cust. ID No. (b) (4)

Bill To
DHS/CBP
WWW.IPP
(b)(6) (b)(7)(C)@cbp.dhs.gov
@cbp.dhs.gov

Ship To
DHS/C
ATTN (b)(6) (b)(7)(C)
PO: 70B04C19F00000802
5971 KINGSTOWNE VILLAGE PKWY., 5TH FLR MR
ALEXANDRIA, VA 22315

P.O. Number	Order Date	Terms	Sales Rep	Via	F.O.B.
70B04C19F00000802	9/24/2019	Net 30	(b)(6) (b)(7)(C)	DROP SHIP	Destination

Line Ite...	Part #	Description	Quantity	Unit Price	Amount
30	P 001	Venntel Portal License per Named User. Named users billed annually. Expansion seats will be pro rated to initial term. Annual queries per user limit (b)(7)(E) calls	(b) (7)(E)	(b) (7)(E), (b) (4)	
40	P 001	Venntel Portal License per Named User. Named users billed annually. Expansion seats will be pro rated to initial term. Annual queries per user limit i (b)(7)(E) calls			
50	S 003	Venntel Portal Suppor (b) (7)(E)			

SEE REVERSE FOR ADDITIONAL TERMS AND CONDITIONS.
(b) (4)

Subtotal	$1,068,317.18
Sales Tax (5.3%)	$0.00
Total	$1,068,317.18
Payments/Credits	$0.00
Balance Due	$1,068,317.18

A HUBZone, WOSB and SWaM CERTIFIED COMPANY
IF YOU HAVE QUESTIONS REGARDING THIS INVOICE PLEASE CONTA (b) (6)
(b) (6)

SDRD8e56

Office of Information and Technology
Service Delivery Requirement Document
FY18 Additional NTC Requirements

CBP Originating Office: OFO
Originating Office Point of Contact (POC) (name): (b)(6) (b)(7)(C)
Originating Office POC phone number: (b)(6) (b)(7)(C)
Date of request: July 3, 2018

Summary

OIT TASPD currently performs a variety of work in support of the National Targeting Center (NTC). NTC has asked that TASPD execute additional funding in FY18 to improve intelligence and targeting capabilities related to screening and vetting of international travelers and those seeking an immigration or travel benefit from the United States Government (USG). It will also support NTC's expanding collaboration with the (b) (7)(E) and National Targeting Center's (NTC) (b) (7)(E) initiative providing systems development and additional equipment in support of two of NTC's primary mission sets; counter-terrorism and counter narcotics.

Detailed Description of Requirement

CBP's targeting enterprise systems process large amounts of regulated trade, travel, and immigration data, surface derogatory information about nefarious individuals and illicit organizations, (b) (7)(E) (b) (7)(E) and provide quality and timely information to multiple stakeholders (b) (7)(E) (b) (7)(E) These systems enable CBP to efficiently screen cargo, passengers, and applicants for national security and public safety risks and streamline information sharing (b) (7)(E) and other interagency partners who adjudicate immigration benefits and/or operate in the same mission spaces. CBP's targeting systems collect and aggregate intelligence and law enforcement information from multiple source systems into a single platform that officers and analysts use to detect and analyze potential threats. The effective aggregation of intelligence and law enforcement information improves targeting, drives more informed screening, vetting, and adjudications and increases operational efficiencies. In order to support all of these efforts, OIT will be investing in the following:

Increase Cloud Migration Support: Moving TASPD applications to the cloud allows a virtualized, highly scalable, and redundant environment, with shared resources that can be tapped on demand and easily scaled in response to changing usage levels.

Additional Analytic Sources via (b) (7)(E) and Venntel: CBP plans to acquire Venntel licenses and access to the (b) (7)(E) database. (b) (7)(E) (b) (7)(E) Subscription, query-based access to commercial data will allow CBP law enforcement officers, agents, and analysts the ability to query (b) (7)(E) (b) (7)(E) for law enforcement related research, to identify trends and patterns, to assist in identifying those who may need additional scrutiny at the border, (b) (7)(E) and assist in intelligence-driven operations related to illicit activity at the border, including (b) (7)(E) (b) (7)(E)

Additional Modeling Efforts: Predictive models serve as decision support tools for CBP Officers (b) (7)(E) (b) (7)(E) (b) (7)(E) OIT will work

with NTC to incorporate additional data streams (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

Hardware: Additional high performance application servers to serve the import cargo and the passenger work flows. This increased capability through investment will enable the NTC to process larger volumes of data efficiently, elevate its screening and vetting capabilities to uniform baseline levels, and streamline information sharing [redacted] to provide more results-based decisions for better-targeted enforcement actions.

Additional Enhancements to IRS-NG and ATS: Additional enhancements based on NTC's priorities will enable CBP to better identify and (b) (7)(E) [redacted] high-risk passengers and cargo by (b) (7)(E) [redacted] (b) (7)(E) [redacted] CBP will also be able to collect more data during encounters, transforming it into useful information for intelligence analysis that inform (b) (7)(E) [redacted] border operations, and other border security mission sets. CBP and other components that leverage its capabilities may share, disseminate, and analyze data collected across the Department for their respective missions. This improved sharing, dissemination and analysis serves as (b) (7)(E) [redacted] (b) (7)(E) [redacted] as individuals proceed along the traveler and immigration continuums.

(b) (7)(E) [redacted]

Funding Source

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

Assumptions

- Out-year costs are for **estimated** future license/software costs and does not include services. If OFO wants to continue use of (b) (7)(E) [redacted] Venntel, or (b) (7)(E) [redacted] ut-year costs will need to be funded.
- This estimate is based on high-level requirements; therefore LOE is notional and subject to change based on NTC input.

OIT Costs

(b) (7)(E) [redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

Detailed description of new investment cost (for each FY as applicable):

The funding will support contractor services associated with the detailed description of work above.

Detailed description of travel: N/A

Detailed description of Operations and Maintenance cost (for each FY as applicable): Out-year costs are for **estimated** future license/software costs and does not include services. If OFO wants to continue use of [redacted] and Venntel, these out-year costs will need to be funded. (amounts included are best estimates, OFO will be required to fund actual vendor costs at time of procurement action.)

Approved by Originating Office: (b)(6) (b)(7)(C) Date 8/6/18

Signature of approval from Originating office: (b)(6) (b)(7)(C) Date 8/6/18

Approved by Originating Office HQ Budget Officer: (b)(6) (b)(7)(C) Date 8/7/18

Signature of approval from originating office HQ Budget Officer (b)(6) (b)(7)(C)

Alignment to CBP Major/non-major investment (to be completed by funding offices budget officer: ____

To be used by OIT below the dotted line

Confirmation that EDME, FS, ENTS, CSD and PSPD have been consulted and that their costs are included:

Directorate	Consulted	Response Date	Costs
EDMED	Yes		
ENTSD	Yes		
FSD	Yes		
CSD	Yes		
BEMSD	Yes		
CSPD	Yes		
PSPD	Yes		
WSPD	Yes		