ORDER FOR SUPPLIES OR SERVICES

CBP-2020-033428-0000458

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

1. DATE OF ORDER: 09/16/2019
2. CONTRACT NO. (if any): HSHQDC-12-D-00013
3. ORDER NO.: 70B04C19F00000798
4. REQUISITION/REFERENCE NO.: 0020108735
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 566658323. 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 BUS NESS (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): 09/20/2020

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) Subscription - Renewal	(b) (7)(E)	AU	(b) (7)(E), (b) (4)		

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: $2,739,507.25

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

OPTIONAL FORM 347 (REV. 2/2012)
Prescr bed by GSA/FAR 48 CFR 53.213 (f)

DATE OF ORDER	CONTRACT NO. (if any)	ORDER NO.	PAGE OF PAGES
09/16/2019	HSHQDC-12-D-00013	70B04C19F00000798	2 4

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, 70B04C19F00000798, is issued against the Department of Homeland Security FirstSource II HSHQDC-12-D-00013 for (b) (7)(E) Annual Subscription 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 # 566658323, dated July 24, 2019, from Unison Buy #983448.

The period of performance will be 9/21/2019 – 9/20/2020.

CONTRACTING OFFICER'S REPRESENTATIVE

Name: (b) (6), (b) (7)(C)
Address:5971 Kingstowne Village Pkwy.th floor mailroom
Alexandria, Virginia, 22315
Tel. #: (b) (6), (b) (7)(C)
Fax. #:
Email: [redacted] cbp.dhs.gov

CONTRACTING OFFICER'S REPRESENTATIVE – ALTERNATE AND IPP APPROVER

Name: (b) (6), (b) (7)(C)
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: 70B04C19F00000798

I.1 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	(b) (7)(E) Subscription - Renewal	(b) (7)(E)	AU	(b) (7)(E), (b) (4)	

Total Funded Value of Award: **$2,739,507.25**

I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	(b) (7)(E)	(b) (7)(E), (b) (4)

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)	09/20/2020

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. FEDERAL ACQUISITION REGULATION (48 CHAPTER 1) CLAUSES

NUMBER TITLE

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 09/21/2019 through 09/20/2020.

[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]

Bill of Materials

Item Description	Quantity
(b) (7)(E) **Licenses Bundle (Brand Name Only) to include:**	
Full Licenses	(b) (7)(E) [redacted]
Pilot Licenses	
(b) (7)(E) [redacted]	
(b) (7)(E) [redacted]	
(b) (7)(E) [redacted]	
Training/Support	
(b) (7)(E) [redacted]	
(b) (7)(E) [redacted]	
(b) (7)(E) [redacted]	

Task Identification Information

2/21/2019

Contract No. DHS First Source II

Customer Name: Targeting & Analysis Systems Program Directorate

70B04C19F00000798

Statement of Work
Department of Homeland Security
Customs & Border Protection (CBP)

1.0 General

In support of US Customs and Border Protection (CBP) mission of securing our nation's borders, the National Targeting Center (NTC) has a need to procure (b) (7)(E) software.

NTC must have the ability to analyze social media in order to gain further insight in accurately identifying and organizing groups of people based on social media postings. The (b) (7)(E) web-based application is (b) (7)(E) [redacted]. The (b) (7)(E) platform generates real-time, actionable intelligence (b) (7)(E) [redacted]

1.1 Scope

The purpose of this order is for the contractor to provide the following software:

Item Description	Quantity
(b) (7)(E) Annual Subscription (in accordance with the attached Bill of Materials)	(b) (7)(E) [redacted]
(b) (7)(E) Annaul Subscription – Pilot Licenses (in accordance with the attached Bill of Materials)	
(b) (7)(E) (in accordance with the attached Bill of Materials)	
(b) (7)(E) (in accordance with the attached Bill of Materials)	
(b) (7)(E) (in accordance with the attached Bill of Materials)	
Training/Support (in accordance with the attached Bill of Materials)	
(b) (7)(E) (in accordance with the attached Bill of Materials)	
(b) (7)(E) (in accordance with the attached Bill of Materials)	
(b) (7)(E) (in accordance with the attached Bill of Materials)	

2.0 Period of Performance

The period of performance for this contract will be 9/21/19-9/20/20.

3.0 Place of Performance

Location: All work required under this order shall be performed by the contractor at Government sites unless otherwise directed by the Government.

4.0 Deliverables

The contractor shall provide the following deliverables: review and concurrence

Deliverable	Due
(b) (7)(E) Annual Subscription (in accordance with the attached Bill of Materials)	Date of Award
(b) (7)(E) Annaul Subscription – Pilot Licenses (in accordance with the attached Bill of Materials)	Date of Award
(b) (7)(E) [redacted] (in accordance with the attached Bill of Materials)	Date of Award
(b) (7)(E) [redacted] (in accordance with the attached Bill of Materials)	Date of Award
(b) (7)(E) [redacted] (in accordance with the attached Bill of Materials)	Date of Award
Training/Support (in accordance with the attached Bill of Materials)	As Required
(b) (7)(E) [redacted] (in accordance with the attached Bill of Materials)	Date of Award
(b) (7)(E) [redacted] (in accordance with the attached Bill of Materials)	Date of Award
(b) (7)(E) [redacted] (in accordance with attached Bill of Materials)	Date of Award

5.0 Type of Contract

Customs and Border Protection will award a firm fixed price task order.

6.0 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.

(1) The minimum requirements are:

i. Name and address of the contractor.
ii. Invoice date and invoice number.
iii. Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number.
iv. Description, quantity, unit of measure, unit price, and extended price of supplies delivered or services performed.
v. 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.
vi. 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).
vii. Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
viii. Taxpayer identification number (TIN).
ix. Electronic funds transfer (EFT) banking information.
x. 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.

7.0 Point of Contact

CONTRACTING OFFICER'S REPRESENTATIVE

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

CONTRACTING OFFICER'S REPRESENTATIVE – ALTERNATE AND IPP APPROVER

Name: (b) (6), (b) (7)(C)
Email: cbp.dhs.gov

Only the contracting officer has the authority to represent the Government in cases where the task order requires a change in the terms and conditions, delivery schedule, scope of work and/or price of the products and/or services under this task order.

8.0 Clauses

The Contractor shall fulfill the duties of this SOW while maintaining full compliance with all terms and conditions of the contract. Please see below for IT security and agency specific clauses applicable to this contract.

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).

DHS Enterprise Architecture Compliance

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

1. All developed solutions and requirements shall be compliant with the HLS EA.

2. All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.

3. 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.

4. 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.

5. 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.

OAST (Office on Accessible Systems and Technology) Compliance

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): Web Forms Applications

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 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 508 requirements for electronic content features and components (including Electronic reports;): Does not apply

Applicable 508 requirements for software features and components (including Web, desktop, server, mobile client applications): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

Applicable 508 requirements for hardware features and components: Does not apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

2. 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.

3. Where ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the Revised 508 Standards consistent with the agency's business needs, in accordance with 36 CFR E202.7. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) 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 and 36 CFR E202.6.

Instructions to Offerors

1. For each commercially available Information and Communications Technology (ICT) item offered through this contract, the Offeror shall provide an Accessibility Conformance Report (ACR). The ACR shall be created using the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed in accordance with all the instructions provided in the VPAT template. Each ACR must

address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All “Supports”, “Supports with Exceptions”, “Does Not Support”, and “Not Applicable” (N/A) responses must be explained in the remarks/explanations column or through additional narrative. The offeror is cautioned to address each standard individually and with specificity, and to be clear whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. The ACR shall provide a description of the evaluation methods used to support Section 508 conformance claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror’s proposed ICT items to validate Section 508 conformance claims made in the ACR.

2. For each commercially available authoring tool offered that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the Offeror shall describe the level of Section 508 compliance supported for the content that can be generated.

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 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. Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have signatory authority.

HSAR Clauses

HSAR Class Deviation 15-01: Safeguarding of Sensitive Information (MAR 2015)

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 13.1, July 27, 2017), 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)

HSAR Class Deviation 15-01 - Information Technology Security and Privacy Training (MAR 2015)

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.

(End of clause)

HSAR – 3052.204-71 - Contractor Employee Access Clause

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) The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
(2) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
(3) 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 Terms and Conditions

(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 to 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 taskings:

- 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

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.

Portfolio Review

Screening/Watchlist/Credentialing

Includes all activities that support the tracking and monitoring of travelers, conveyances and cargo crossing U.S. borders, and traffic pattern analysis, database (Federal, State, and Local) linking and querying, and 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.

ORDER FOR SUPPLIES OR SERVICES

CBP-2020-033428-0000495

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

1. DATE OF ORDER: 8/5/2020
2. CONTRACT NO. (if any): HSHQDC-13-D-00022
3. ORDER NO.: 70B04C20F00000914
4. REQUISITION/REFERENCE NO.: 0020115293
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: GOVPLACE
b. COMPANY NAME:
c. STREET ADDRESS: 11111 SUNSET HILLS RD STE 200
d. CITY: RESTON
e. STATE: VA
f. ZIP CODE: 20190-5373

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 he 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 BUS NESS (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): 09/27/2020

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	Venntel	(b) (7)(E)	AU	(b) (7)(E), (b) (4)		

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

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

17(i) GRAND TOTAL: $475,944.49

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

OPTIONAL FORM 347 (REV. 2/2012)
Prescr bed by GSA/FAR 48 CFR 53.213 (f)

DATE OF ORDER	CONTRACT NO. (if any)	ORDER NO.	PAGE OF PAGES
8/5/2020	HSHQDC-13-D-00022	70B04C20F00000914	2 4

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, 70B04C20F00000914, is issued against the Department of Homeland Security FirstSource II Contract HSHQDC-13-D-00022 for Venntel Software in support of Targeting and Analysis Systems Program Directorate's (TASPD) The Statement of Work will be provided with the Distribution email.

Reference Bid # 567947216, from DHS Marketplace (Unison).

The Period of Performance for 70B04C20F00000914: 9/25/2020 - 9/14/2021

The Contracting Officer's Representative for this order is:
(b) (6), (b) (7)(C) [redacted]@CBP.DHS.GOV

The Budget (IPP Approver) for this order is:
(b) (6), (b) (7)(C) [redacted] cbp.dhs.gov

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

ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: 70B04C20F00000914

I.1 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	Venntel	(b) (7)(E)	AU	(b) (7)(E), (b) (4)	

Total Funded Value of Award: **$475,944.49**

I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	(b) (7)(E)	(b) (7)(E), (b) (4)

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)	09/27/2020

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. FEDERAL ACQUISITION REGULATION (48 CHAPTER 1) CLAUSES

NUMBER TITLE

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 09/25/2020 through 09/14/2021.

[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]

70B04C20F00000914

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 Venntel software. This software is in support of mission critical decision making by providing access to commercially available, multi-sourced, validated, location marketing data via custom geolocation data research requests.

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

Item Description	Quantity
Venntel (RENEWAL) *In accordance with the attached Bill of Materials	(b) (7)(E) [redacted]
Venntel (NEW) *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 9/25/20-9/14/21.

1.2 PLACE OF PERFORMANCE

Place of performance will be at government facilities.

2.0 SPECIFIC TASKS

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: (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

IPP APPROVER
Name: (b) (6), (b) (7)(C)
Address: 5971 Kingstowne Village Pkwy.
5th floor mailroom
Alexandria, VA 22315
Tel. #: (b) (6), (b) (7)(C)
Fax. #:
Email: @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).

DHS Enterprise Architecture Compliance

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.

70B04C20F00000914

Instructions to Offerors

1. For each commercially available Information and Communications Technology (ICT) item offered through this contract, the Offeror shall provide an Accessibility Conformance Report (ACR). The ACR shall be created using the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed in accordance with all the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Supports", "Supports with Exceptions", "Does Not Support", and "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. The offeror is cautioned to address each standard individually and with specificity, and to be clear whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. The ACR shall provide a description of the evaluation methods used to support Section 508 conformance claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror's proposed ICT items to validate Section 508 conformance claims made in the ACR.

2. For each commercially available authoring tool offered that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the Offeror shall describe the level of Section 508 compliance supported for the content that can be generated.

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:**

70B04C20F00000914
"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.

U.S. Customs and Border Protection

Office of Information and Technology

Service Delivery Requirements Document

Commercial Telemetry Data Pilot - Venntel Portal Access

CBP Originating Office: Office of the Commissioner

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

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

Date of Request: April 16, 2020

Detailed Description of Requirement:

U.S. Customs and Border Protection (CBP) INVNT office requires access to commercial telemetry data as part of a commercial telemetry data pilot. The pilot relates to the use of location information derived from commercially available telemetry data used in the advertising and marketing ecosystem. This commercial telemetry data, associated with the Advertising Identifier, contains location information captured by applications (apps) on modern mobile smart devices, such as smartphones.

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

Item Description Quantity

Venntel portal access for a named user (b) (7)(

The period of performance will be 9/25/20-9/24/21

Historical Information/Background on Requirement:

N/A

Funding Source:

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

Group	Type	FY 2020	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025
TASPD	Gov't Position	(b) (7)(E)					
TASPD	New Investment						
TASPD	O&M						
	Total						

Detailed Description of Government Position Cost:

TASPD

Office of the Commissioner

N/A

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

TASPD

Office of the Commissioner

TASPD will provide procurement support to establish service from the vendor. Funds will be used to establish a firm fixed price contract for licensing fees for Venntel Portal portal access.

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

TASPD

Office of the Commissioner

N/A. This SDR funds a one year FFP contract. If it is determined that out year support is required, a new SDR would be prepared.

Originating Office Approval:

	Name	Date
Originating Office Signature:	(b) (6), (b) (7)(C)	6/3/2020
	Signature	Date

HQ Budget Officer Approval:

	Name	Date
HQ Budget Officer Signature:	(b) (6), (b) (7)(C)	
	Signature	Date

Alignment to CBP Major/non-major investment:

Approval History:

Approver:	**Status:**	**Approved By:**	**Approval Date:**
EDMED	Approved without Budget	(b) (6), (b) (7)(C)	May 14, 2020
ENTSD	Approved without Budget		May 13, 2020
FSD	No Response - Approved	SDR System User	May 15, 2020
CSD	No Response - Approved	SDR System User	May 15, 2020
FMD	No Response - Approved	SDR System User	May 15, 2020
CTO	Approved	(b) (6), (b) (7)(C)	May 22, 2020
DAC	Approved		June 1, 2020

Expiration Date:

Justification for Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

Date: 6/14/19 PR Number: 20111511

1. Agency and Contracting Activity. Identification of the agency and the contracting activity, and specific identification of the document as a "Justification for an Exception to Fair Opportunity."

U.S. Customs and Border Protection (CBP), Information and Technology Contracting Division (ITCD) prepared this justification for a brand name exception to fair opportunity.

2. Nature and/or description of the action being approved.

CBP, Office of Information and Technology (OIT), Targeting and Analysis Systems Program Directorate (TASPD) requires the purchase of (b) (7)(E) tools in support of the National Targeting Center's (NTC) analysts. Pursuant to FAR 16.505(a)(4), this requirement is peculiar to specific manufacturers ((b) (7)(E) (b) (7)(E) and Venntel) and compeititon will be limited to authorized resellers available on DHS FirstSource II.

3. A description of the supplies or services required to meet the agency's need (including the estimated value).

The Targeting and Analysis Systems Program Directorate (TASPD) requires the procurement of (b) (7)(E) tools in an operation environment in support of a proof of concept. The supplies required under this order include the following:

- (b) (7)(E)
-
- Venntel

This software is critical to the ongoing operations in support of the CBP mission of managing and securing the nation's borders.

The period of performance is 12 months and the estimated total value of this requirement is (b) (7)(E), (b) (5)

4. Identify the exception to fair opportunity and supporting rationale. Only one awardee is capable of providing the supplies required at the level of quality required because the supplies ordered are unique or highly specialized pursuant to FAR16.505(b)(2)(i)(B) and is an item peculiar to one manufacturer:

Justification for Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

OA/PD intends to procure a brand name specification for (b) (7)(E) and Venntel software and support in accordance with FAR 16.505(a)(4)(i) or (ii). The exception is based on FAR 16.505(b)(2)(i)(B), only one source is capable of providing each of the software tools because the licenses are highly specialized and are brand name items peculiar to the Original Equipment Manufacturers (OEM). Each product is unique in the marketplace in the following area:

(b) (7)(E)

(b) (7)(E)

Justification for Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

(b) (7)(E)

- Venntel:

The Venntel web-based portal application is a (b) (7)(E) (b) (7)(E) processing technology reliably filters, aggregates, and categorizes location data for superior data reliability and transparency. The Venntel platform supports mission-critical decision making by providing access to commercially available, (b) (7)(E) (b) (7)(E) Venntel is the sole provider of updates and maintenance to the web-based application and data processing platform. These services are completely web-based and do not require ICE/CIO installation or hardware purchases.

The Venntel platform (b) (7)(E) (b) (7)(E) (b) (7)(E) Venntel is unique among its competitors in that it uses a Venntel-specific, proprietary platform that (b) (7)(E) (b) (7)(E) (b) (7)(E) While its competitors offer (b) (7)(E) (b) (7)(E) (b) (7)(E) Venntel provides bespoke solutions tailored to the unique requirements of agencies operating in the law enforcement mission spaces. (b) (7)(E), (b) (5)

CBP, Office of Information and Technology (OIT), National Targeting Center (NTC) (b) (7)(E), (b) (5)

Justification for Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

CBP continuously conducts market research on other products commercially available. The results of the market research indicate that these products are currently unique in their capabilities in the marketplace. (b) (5) [redacted]

In addition, this requirement was posted on the Acquisition Planning Forecast System (APFS), #2018044789. TASPD has received no interest from other potential vendors to date.

5. Determination by the contracting officer that the anticipated cost to the Government will be fair and reasonable.

By competing the requirement utilizing an established DHS FirstSource II contract holder, it is anticipated that there will be adequate price competition upon issuance of the Request for Quote (RFQ). Furthermore, the final price will be analyzed against the Independent Government Cost Estimate (IGCE) and previous year expenditures for similar products/services. As an order placed against the DHS strategic sourcing vehicle, pricing has been independently determined to be fair and reasonable by DHS at the time of the IDIQ contract award. These combined factors provide sufficient information in determining that the anticipated cost to the Government will be fair and reasonable.

6. Any other facts supporting the justification.

This product is critical to the ongoing operations in support of CBP's mission of managing and securing the nation's borders.

7. A statement of the actions, if any, the agency may take to remove or overcome any barriers that led to the exception to fair opportunity before any subsequent acquisition for the supplies or services is made.

With regard to the analytics tools, there are no planned actions at this time that are feasible or in the best interest of the Government that would remove or overcome any barriers to competition. CBP/OIT/TASPD regularly conducts market research to identify any additional products that may have the necessary capabilities to meet CBP's need. (b) (5) [redacted]

8. DHS intends to post this requirement on FedBizOpps pursuant to FAR 16.505(b)(2)(ii)(D).

Justification for Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

9. Technical/Requirements Personnel Certification.

Pursuant to FAR 16.505(b)(2)(ii)(B)(9), I certify that this requirement meets the Government's minimum need and that the supporting data, which form a basis for the justification, are accurate and complete.

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

Technical Representative/COR _____ Date

10. Contracting Officer Certification and/or Approval *

Pursuant to FAR 16.505(b)(2)(ii)(B)(8), I certify that this justification is accurate and complete to the best of my knowledge and belief and hereby determine that the circumstances for an

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

Not exceeding $700,000 _____ Date
Contracting Officer

*Note: In accordance with FAR 16.505(b)(2)(ii)(C)(1), proposed orders with an estimated value exceeding the simplified acquisition threshold, but not exceeding $650,000, the ordering activity contracting officer's certification that the justification is accurate and complete to the best of the ordering activity contracting officer's knowledge and belief will serve as approval. For OPO, the contracting officer should sign each justification prior to approval by the next higher level (e.g., Competition Advocate, HCA, and/or CPO).

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

Over $700,000 but not exceeding $13.5 million _____ Date
Component Competition Advocate

Justification for Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

Date: 2/11/2020 PR Number: 20115293

1. Agency and Contracting Activity. Identification of the agency and the contracting activity, and specific identification of the document as a "Justification for an Exception to Fair Opportunity."

U.S. Customs and Border Protection (CBP), Information and Technology Contracting Division (ITCD) prepared this justification for a brand name exception to fair opportunity.

2. Nature and/or description of the action being approved.

CBP, Office of Information and Technology (OIT) requires the purchase of (b) (7)(E) (b) (7)(E) tools in support of analysts' mission critical work. Pursuant to FAR 16.505(a)(4), this requirement is peculiar to a specific manufacturer, Venntel, and competition will be limited to authorized resellers available on DHS FirstSource II.

3. A description of the supplies or services required to meet the agency's need (including the estimated value).

OIT requires the procurement of (b) (7)(E) tools in an operation environment. The supplies required under this order include the following:

- Venntel

This software is critical to the ongoing operations in support of the CBP mission of managing and securing the nation's borders.

The period of performance is 12 months and the estimated total value of this requirement is (b) (7)(E), (b) (5)

4. Identify the exception to fair opportunity and supporting rationale. Only one awardee is capable of providing the supplies required at the level of quality required because the supplies ordered are unique or highly specialized pursuant to FAR16.505(b)(2)(i)(B) and is an item peculiar to one manufacturer:

OA/PD intends to procure a brand name specification for Venntel software and support in accordance with FAR 16.505(a)(4)(i) or (ii). The exception is based on FAR 16.505(b)(2)(i)(B), only one source is capable of providing the software tool because the license is highly specialized and is a brand name item peculiar to the Original Equipment Manufacturer (OEM).

The Venntel web-based portal application is a (b) (7)(E) (b) (7)(E) Venntel's proprietary processing

technology reliably filters, aggregates, and categorizes location data for superior data reliability and transparency. The Venntel platform supports mission-critical decision making by providing access to commercially available. (b) (7)(E) [redacted] (b) (7)(E) [redacted]. Venntel is the sole provider of updates and maintenance to the web-based application and data processing platform. These services are completely web-based and do not require ICE/CIO installation or hardware purchases.

The Venntel platform (b) (7)(E) [redacted] (b) (7)(E) [redacted] Venntel is unique among its competitors in that it uses a Venntel-specific, proprietary platform that (b) (7)(E) [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted] While its competitors offer (b) (7)(E) [redacted] (b) (7)(E) [redacted] Venntel provides bespoke solutions tailored to the unique requirements of agencies operating in the law enforcement mission spaces. (b) (7)(E), (b) (5) [redacted]

CBP continuously conducts market research on other products commercially available. The results of the market research indicate that these products are currently unique in their capabilities in the marketplace. (b) (5) [redacted]

5. Determination by the contracting officer that the anticipated cost to the Government will be fair and reasonable.

By competing the requirement utilizing an established DHS FirstSource II contract holder, it is anticipated that there will be adequate price competition upon issuance of the Request for Quote (RFQ). Furthermore, the final price will be analyzed against the Independent Government Cost Estimate (IGCE) and previous year expenditures for similar products/services. As an order placed against the DHS strategic sourcing vehicle, pricing has been independently determined to be fair and reasonable by DHS at the time of the IDIQ contract award. These combined factors provide sufficient information in determining that the anticipated cost to the Government will be fair and reasonable.

6. Any other facts supporting the justification.

This product is critical to the ongoing operations in support of CBP's mission of managing and securing the nation's borders.

Justification for Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

7. A statement of the actions, if any, the agency may take to remove or overcome any barriers that led to the exception to fair opportunity before any subsequent acquisition for the supplies or services is made.

With regard to the Venntel tool, there are no planned actions at this time that are feasible or in the best interest of the Government that would remove or overcome any barriers to competition. CBP/OIT regularly conducts market research to identify any additional products that may have the necessary capabilities to meet CBP's need.

8. DHS intends to post this requirement on FedBizOpps pursuant to FAR 16.505(b)(2)(ii)(D).

9. Technical/Requirements Personnel Certification.

Pursuant to FAR 16.505(b)(2)(ii)(B)(9), I certify that this requirement meets the Government's minimum need and that the supporting data, which form a basis for the justification, are accurate and complete.

_____ _____
Technical Representative/COR Date

10. Contracting Officer Certification and/or Approval *

Pursuant to FAR 16.505(b)(2)(ii)(B)(8), I certify that this justification is accurate and complete to the best of my knowledge and belief and hereby determine that the circumstances for an

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

_____
Not exceeding $700,000 Date
Contracting Officer

Attachment 6
U.S. Customs and Border Protection
Justification for a Brand Name Exception to Fair Opportunity (JEFO) – FAR 16.505(a)(4)
Above the micro-purchase threshold but not exceeding the SAT

Date: 08/28/2020 PR Number: ___20120660_____

1. **Agency and Contracting Activity**.

The Department of Homeland Security (DHS), United States Customs and Border Protection (CBP), Office of Acquisition – Procurement Directorate (OA/PD) prepared this justification for a brand name exception to fair opportunity.

2. Nature and/or description of the action being approved.

CBP intends to use a brand-name specification pursuant to *FAR 16.505(a)(4)* for the procurement of (b) (7)(E) Venntel licenses and (b) (7)(E) CBP intends to award a firm-fixed-price delivery order competed among authorized resellers of Venntel under the DHS FirstSource II multiple award indefinite-delivery/indefinite quantity (IDIQ) contract vehicle HSHQDC13D00020.

3. A description of the supplies or services required to meet the agency's need (including the estimated value).

Venntel's proprietary processing technology reliably filters, aggregates, and categorizes location data for superior data reliability and transparency. The web based platform supports CBP operators and analysts across the enterprise in mission-critical decision making by providing access to commercially available, (b) (7)(E) (b) (7)(E) CBP has used Venntel for approximately (b) (7)(E) to (b) (7)(E)

License Acquisition: Procurement of (b) (7)(E) Venntel licenses and (b) (7)(E) (b) (7)(E) in accordance with the Statement of Work (SOW).

Period of performance: 9/21/20 - 9/20/21 (12 months)

Total Estimated Value: (b) (7)(E), (b) (5)

Period	Unit Price	Total
Base Year - 12 mo.	(b) (7)(E), (b) (5), (b) (4)	(b) (7)(E), (b) (5)
	Total	(b) (7)(E), (b) (5)

4. Identification of the exception to fair opportunity and supporting rationale, including a demonstration that the proposed contractor's unique qualifications or the nature of the acquisition requires use of the exception cited.

Attachment 6
U.S. Customs and Border Protection
Justification for a Brand Name Exception to Fair Opportunity (JEFO) – FAR 16.505(a)(4)
Above the micro-purchase threshold but not exceeding the SAT

This procurement is in accordance with FAR 16.505(a)(4)(ii) - Use of brand name specification. The exceptions at FAR 16.505(b)(2) do not apply as this is a brand-name justification; however, the justification format at FAR 16.505(b)(2)(ii)(B) applies and is modified to reflect a brand-name justification.

Rationale:

CBP intends to limit fair opportunity to authorized resellers of Venntel under the DHS FirstSource II IDIQ contract vehicle HSHQDC13D00020. Venntel provides CBP a critical resource in support of national security and law enforcement requirements across all threats and operational environments. Venntel is currently being used by (b) (7)(E) (b) (7)(E) (b) (7)(E) Venntel's differentiator is its

CBP has conducted market research and tested other commercially available telemetry platforms ((b) (7)(E) . (b) (7)(E), (b) (5) (b) (7)(E)

5. Determination by the contracting officer that the anticipated cost to the Government will be fair and reasonable.

By competing the requirement among DHS FirstSource II contract holders, it is anticipated that there will be adequate price competition upon issuance of the Request for Quotes (RFQ). Furthermore, the final price will be analyzed against the Independent Government Cost Estimate (IGCE) and previous year expenditures for similar products/services. As an order placed against the DHS strategic sourcing vehicle, pricing was independently determined to be fair and reasonable by DHS at the time of the IDIQ contract award. These combined factors provide sufficient information to enable the Government to reasonably expect the cost to the Government will be fair and reasonable.

6. Any other facts supporting the justification.

Since February 2016, CBP's National Targeting Center – Counter Network Division - (b) (7)(E) (b) (7)(E) (NTC-CND (b) (7)(E) has researched (b) (7)(E) publicly and ology enabled solutions (tools, capabilities, and datasets) relevant to CBP's mission, e.g. screening and vetting of passengers and cargo. Of the (b) (7)(E) echnology-enabled solutions that (b) (7)(E) has assessed to date, Venntel meets or exceeds certain mission critical requirements. As this domain is extremely dynamic, (b) (7)(E) ontinues to identify,

Attachment 6
U.S. Customs and Border Protection
Justification for a Brand Name Exception to Fair Opportunity (JEFO) – FAR 16.505(a)(4)
Above the micro-purchase threshold but not exceeding the SAT

research, and evaluate new and existing tools, capabilities, and datasets as part of its on-going market research initiative. Continued acquisition of this software is essential to national security and failure to procure Venntel may adversely impact CBP's ability to target and vet threats to the U.S. Homeland.

7. A statement of the actions, if any, the agency may take to remove or overcome any barriers that led to the exception to fair opportunity before any subsequent acquisition for the supplies or services is made.

CBP/OFO/NTC/CND (b) (7)(E) regularly conducts market research to identify and review any commercial platforms or datasets that meet CBP mission needs. CBP's current approach is to acquire and deploy a suite of applications used by CBP operators and analysts in the field. The suite includes both (b) (7)(E) [redacted] (b) (7)(E) [redacted] In whole, CBP's complementary capabilities enable [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted] CBP has identified Venntel as a critical element to support this approach at present, and will continue to work to identify other alternatives CBP might incorporate into its suite of solutions to achieve its targeting mission.

8. CBP intends to provide the justification with the solicitation pursuant to FAR 16.505(a)(4)(iii)(A)(2).

9. Technical/Requirements Personnel Certification:

Pursuant to FAR 16.505(b)(2)(ii)(B)(9), I certify that this requirement meets the Government's minimum need and that the supporting data, which form a basis for the justification, are accurate and complete.

(b) (6), (b) (7)(C) [redacted]

Technical Representative/COR _____ Date

10. Contracting Officer Certification and Approval: *

Pursuant to FAR 16.505(b)(2)(ii)(B)(8), I certify that this justification is accurate and complete to the best of my knowledge and belief and hereby determine that the circumstances for an exception to fair opportunity exist:

(b) (6), (b) (7)(C) [redacted]

8/28/2020
Date

Attachment 6
U.S. Customs and Border Protection
Justification for a Brand Name Exception to Fair Opportunity (JEFO) – FAR 16.505(a)(4)
Above the micro-purchase threshold but not exceeding the SAT

*Note: In accordance with FAR 16.505(b)(2)(ii)(C)(2), proposed orders with an estimated value exceeding $700,000, but not exceeding $13.5 million, justification must be approved by the advocate for competition of the activity placing the order, or by an official named in FAR 16.505(b)(2)(ii)(C)(3) or (4). For CBP, the contracting officer should sign each justification prior to approval by the next higher level (e.g., Competition Advocate, HCA, and/or CPO).

U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO) – FAR 16.505(a)(4)
Exceeding the SAT

Date: 6/5/19 PR Number: 20108735

1. Agency and Contracting Activity. Identification of the agency and the contracting activity, and specific identification of the document as a "Justification for an Exception to Fair Opportunity."

The Department of Homeland Security, Customs and Border Protection, Information and Technology Contracting Division (ITCD) prepared this justification for a brand name exception to fair opportunity.

2. Nature and/or description of the action being approved.

CBP, Office of Information and Technology (OIT) requires the purchase of (b) (7)(E) software and maintenance. Pursuant to FAR 16.505(a)(4), this requirement is peculiar to one manufacturer, (b) (7)(E) While multiple vendors on DHS FirstSource II will be able to compete for this requirement, it is proprietary to one manufacturer, (b) (7)(E).

3. A description of the supplies or services required to meet the agency's need (including the estimated value).

The Targeting and Analysis Systems Program Directorate (TASPD), within ES-OIT, and the National Targeting Center (NTC) require the procurement of (b) (7)(E) software and maintenance. (b) (7)(E) is the name of the Original Equipment Manufacturer (OEM). (b) (7)(E) offers a variety of products and services. (b) (7)(E) is one of the offerings from (b) (7)(E) and is required under this order as follows:

Item Description	Quantity
(b) (7)(E) **Licenses Bundle (Brand Name Only) to include:**	
Full Licenses	(b) (7)(E)
Pilot Licenses	
(b) (7)(E)	
Training/Support	
(b) (7)(E)	

The estimated total value of this requirement is (b) (7)(E), (b) (5)

4. Identify the exception to fair opportunity and supporting rationale, including a demonstration that the proposed contractor's unique qualifications or the nature of the acquisition requires use of the exception cited. *[Select one and explain rationale below]*

U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO) – FAR 16.505(a)(4)
Exceeding the SAT

_____FAR 16.505(b)(2)(i)(A). The agency need for the supplies or services is so urgent that providing a fair opportunity would result in unacceptable delays.

_____X__FAR 16.505(b)(2)(i)(B). Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized. *[The justification must demonstrate that the proposed contractor's unique qualifications or the nature of the acquisition requires use of the exception cited. If you are preparing a brand name justification, see the requirements at FAR 16.505(a)(4)(i) and (ii) and explain rationale for brand name if an item is peculiar to one manufacturer.]*

_____FAR 16.505(b)(2)(i)(C). The order must be issue on a sole-source basis in the interest of economy and efficiency because it is a logical follow-on to an order already issued under the contract, provided that all awardees were given a fair opportunity to be considered for the original order. *[For logical follow-on, the rationale shall describe why the relationship between the initial order and the follow-on is logical (e.g., in terms of scope, period of performance, or value).]*

_____FAR 16.505(b)(2)(i)(D). It is necessary to place an order to satisfy a minimum guarantee.

_____FAR 16.505(b)(2)(i)(E). For orders exceeding the simplified acquisition threshold, a statute expressly authorizes or requires that the purchase be made from a specified source.

Rationale:

A brand name specification is intended for the procurement of (b) (7)(E) software in accordance with FAR 16.505(b)(2)(i)(B). The exception is based on FAR 16.505(b)(2)(i)(B), only one source is capable of providing the (b) (7)(E) software required at the level of quality required because the supplies or servies ordered are unique or highly specialized and is a brand name item peculiar to the Original Equipment Manufacturer (OEM).

CBP intends to procure a brand name specification for (b) (7)(E) subscription renewals and support. The (b) (7)(E) software and support are peculiar to the Original Equipment Manufacturer (OEM), (b) (7)(E). The (b) (7)(E) product will provide CBP with additional resources to identify potential risks using an advanced statistical approach.

The brand name must be used because (b) (7)(E) is the only company with the capability to (b) (7)(E) (b) (7)(E). Procuring an alternate product other than (b) (7)(E) software will be to the detriment of the Government, as other products on the market do not adequately meet CBP's needs. Additionally, this requirement is for the renewal of the maintenance on existing software within CBP; TASPD and the National Targeting Center (NTC)

U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO) – FAR 16.505(a)(4)
Exceeding the SAT

analytics teams require the use of this product to ensure continuity of current operations as the software has been in place for (b) (7)(E) years. Only (b) (7)(E) and its authorized partners are eligible to perform maintenance on (b) (7)(E) software. Finally, transitioning to a different product is not possible due to the lack of other capable products in the market, as well as a lack of available dedicated resources to replicate the capabilities provided by (b) (7)(E). To remove this software and use a new product would require complete replacement with a significant increase in cost. This involves purchasing and configuring the new software, training on how to use the new product, and implementation.

CBP has conducted market research on other products commercially available ((b) (7)(E) (b) (7)(E)). The results of the market research, further detailed in the Market Research Report, indicate that no other companies currently have the same capabilities to be able to provide this (b) (7)(E) and analysis at the level required to meet CBP's mission. The proprietary capabilities of (b) (7)(E) related to the law enforcement and intelligence missions include:

(b) (7)(E)

This requirement was posted on the Acquisition Planning Forecast System (APFS), #2018044786. CBP has received no interest from other potential vendors.

5. Determination by the contracting officer that the anticipated cost to the Government will be fair and reasonable.

By competing the requirement utilizing an established DHS FirstSource II contract holder, it is anticipated that there will be adequate price competition upon issuance of the Request for Proposals (RFP). Furthermore, the final price will be analyzed against the Independent Government Cost Estimate (IGCE) and previous year expenditures for similar products/services. As an order placed against the DHS strategic sourcing vehicle, pricing has been independently determined to be fair and reasonable by DHS at the time of the Indefinite Delivery/Indefinite Quantity (IDIQ) contract award. These combined factors provide sufficient information in determining that the anticipated cost to the Government will be fair and reasonable.

6. Any other facts supporting the justification.

Market research has concluded that the (b) (7)(E) software is the only solution that provides the capabilities required by the analysts at the National Targeting Center.

U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO) – FAR 16.505(a)(4)
Exceeding the SAT

7. A statement of the actions, if any, the agency may take to remove or overcome any barriers that led to the exception to fair opportunity before any subsequent acquisition for the supplies or services is made.

As the marketplace continues to evolve, CBP Office of Information and Technology (OIT) will continue to monitor and conduct market research for additional products, manufacturers, and solutions that can sufficiently meet the aforementioned critical mission capabilities.

8. CBP will post this justification with the solicitation pursuant to FAR 16.505(a)(4)(iii).

9. Technical/Requirements Personnel Certification:

Pursuant to FAR 16.505(b)(2)(ii)(B)(9), I certify that this requirement meets the Government's minimum need and that the supporting data, which form a basis for the justification, are accurate and complete.

(b) (6), (b) (7)(C) 7/12/2019

Technical Representative/COR Date

10. Contracting Officer Certification and Approval: *

Pursuant to FAR 16.505(b)(2)(ii)(B)(8), I certify that this justification is accurate and complete to the best of my knowledge and belief and hereby determine that the circumstances for an exception to fair opportunity exist:

(b) (6), (b) (7)(C) 7/16/2019

Contracting Officer Date

*Note: In accordance with FAR 16.505(b)(2)(ii)(C)(1), proposed orders with an estimated value exceeding the simplified acquisition threshold, but not exceeding $700,000, the ordering activity contracting officer's certification that the justification is accurate and complete to the best of the ordering activity contracting officer's knowledge and belief will serve as approval. For CBP, the contracting officer should sign each justification prior to approval by the next higher level (e.g., Competition Advocate, HCA, and/or CPO).

11. Chief Council Review (Per HSAM 3006.304-70 – Above the SAT)

Name (print)_____

Signature:_____ _____

U.S. Customs and Border Protection
Justification for Exception to Fair Opportunity (JEFO) – FAR 16.505(a)(4)
Exceeding the SAT

Date

► JEFO Approvals:

12. COMPETITION ADVOCATE (Per FAR 16.505(b)(2)(ii)(C)(2) - Above $700,000)

☒ Approved ☐ Disapproved

Name (Print): (b) (6), (b) (7)(C)
Competition Advocate

Signature: (b) (6), (b) (7)(C) Date: _____

OPOAM 3016.505-90(a)(2)(iv)
Justification for Brand Name Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

Date: 8/1/18 PR Number: 20107297

1. Agency and Contracting Activity. Identification of the agency and the contracting activity, and specific identification of the document as a "Justification for an Exception to Fair Opportunity."

U.S. Customs and Border Protection (CBP), Information and Technology Contracting Division (ITCD) proposed to enter into a contract on a basis other than full and open competition.

2. Nature and/or description of the **action** being approved.

CBP, Office of Information and Technology (OIT), Targeting and Analysis Systems Program Directorate (TASPD) requires the purchase o (b) (7)(E) tools in support of the National Targeting Center's (NTC) analysts. Pursuant to FAR 16.505(a)(4), this requirement is peculiar to specific manufacturer (b) (7)(E) , and Venntel).

3. A description of the supplies or services required to meet the agency's need (including the estimated value).

The Targeting and Analysis Systems Program Directorate (TASPD) requires the procurement o (b) (7)(E) tools in an operation environment in support of a proof of concept. The supplies required under this order include the following:

- (b)(7)(E)
-
-
- Venntel

This software is critical to the ongoing operations in support of the CBP mission of managing and securing the nation's borders.

The estimated total value of this requirement i (b) (7)(E), (b) (5)

4. Identify the exception to fair opportunity and supporting rationale. Only one awardee is capable of providing the supplies required at the level of quality required because the supplies ordered are unique or highly specialized pursuant to FAR16.505(b)(2)(i)(B) and is an item peculiar to one manufacturer:

(b) (7)(E) The exception is based on FAR

16.505(b)(2)(i)(B), only one source is capable of providing each of the software tools because the licenses are highly specialized and are brand name items peculiar to the Original Equipment Manufacturers (OEM). Each product is unique in the marketplace in the following area:

- (b) (7)(E) [redacted]
- [redacted]
- [redacted]; and
- Venntel provides emerging analytics capabilities and has relationships with other DHS partners who have provided Authority to Test (ATO) reviews deeming Venntel unique in the market.

CBP, Office of Information and Technology (OIT), National Targeting Center (NTC) (b) (5) [redacted].

CBP continuously conducts market research on other products commercially available. The results of the market research indicate that these products are currently unique in their capabilities in the marketplace (b) (5) [redacted]

NTC has a significant need for software with the functionality listed in the attached Bill of Materials, Statement of Work, and this Justification. The requirement for functionality and compatibility within CBP will impact the ability to compete this acquisition.

In addition, this requirement was posted on the Acquisition Planning Forecast System (APFS), #2018043284. TASPD has received no interest from other potential vendors to date.

5. Determination by the contracting officer that the anticipated cost to the Government will be fair and reasonable.

By competing the requirement utilizing an established DHS FirstSource II contract holder, it is anticipated that there will be adequate price competition upon issuance of the Request for Quote (RFQ). Furthermore, the final price will be analyzed against the Independent Government Cost Estimate (IGCE) and previous year expenditures for similar products/services. As an order placed against the DHS strategic sourcing vehicle, pricing has been independently determined to be fair and reasonable by DHS at the time of the IDIQ contract award. These combined factors provide sufficient information in determining that the anticipated cost to the Government will be fair and reasonable.

6. Any other facts supporting the justification.

OPOAM 3016.505-90(a)(2)(iv)
Justification for Brand Name Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

This product is critical to the ongoing operations in support of CBP's mission of managing and securing the nation's borders.

7. A statement of the actions, if any, the agency may take to remove or overcome any barriers that led to the exception to fair opportunity before any subsequent acquisition for the supplies or services is made.

With regard to the analytics tools, there are no planned actions at this time that are feasible or in the best interest of the Government that would remove or overcome any barriers to competition. CBP/OIT/TASPD regularly conducts market research to identify any additional products that may have the necessary capabilities to meet CBP's need (b) (5) [redacted].

Each software is proprietary to its manufacturer; however, they are available via resellers on DHS FirstSource II.

8. DHS intends to post this requirement on FedBizOpps pursuant to FAR 16.505(b)(2)(ii)(D).

9. Technical/Requirements Personnel Certification.

Pursuant to FAR 16.505(b)(2)(ii)(B)(9), I certify that this requirement meets the Government's minimum need and that the supporting data, which form a basis for the justification, are accurate and complete.

_____ _____
Technical Representative/COR Date

10. Contracting Officer Certification and/or Approval *

Pursuant to FAR 16.505(b)(2)(ii)(B)(8), I certify that this justification is accurate and complete to the best of my knowledge and belief and hereby determine that the circumstances for an exception to fair opportunity exist:

_____ _____
Not exceeding $700,000 Date
Contracting Officer

*Note: In accordance with FAR 16.505(b)(2)(ii)(C)(1), proposed orders with an estimated value exceeding the simplified acquisition threshold, but not exceeding $650,000, the ordering activity contracting officer's certification that the justification is accurate and complete to the best of the ordering activity contracting officer's knowledge and belief will serve as approval. For OPO, the

CBP-2020-033428-0000548

contracting officer should sign each justification prior to approval by the next higher level (e.g., Competition Advocate, HCA, and/or CPO).

_____ _____

Over $700,000 but not exceeding $13.5 million Date
Component Competition Advocate

Attachment 2
U.S. Customs and Border Protection
Sole Source Determination
For actions above the micro-purchase threshold but not exceeding the SAT

Date: _9-1-2020___ PR Number: _ 20120481_

1. Nature and/or description of the item/service being procured and anticipated cost:

There are over 350 million mobile devices in the United States in use today, and that number is growing exponentially as more people purchase mobile devices every day. Mobile devices, in particular cellphones, are used by criminals and criminal organizations for illicit operations. (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) does not have the capability of utilizing existing technology to capture this information (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) access to Venntel's Mobile Location Platform. It is a proprietary software platform that analyzes billions of commercially-available location signals to provide insight into digital device locations and movement patterns. This software platform is also commonly referred to as Venntel. Price: (b) (7)(E), (b) (4)

R 13.106-1(b)(1)(i) and (ii). *(Check one and explain below):*

_____ Only one source reasonably available.
_____ Urgent and compelling circumstances exists.
_____ Exclusive licensing agreement exists.
_____ Brand name. If the brand name requirement applies to a portion of the procurement, please identify that portion.
_____ Industrial Mobilization
_____x____ Other. Explain:

A description of the market research conducted among schedule holders, if applicable, and the results or a statement of the reason market research was not conducted.

(b) (5)
(b) (5) While the mechanics and nature of Venntel are extremely confidential and proprietary, the vendor has been very forthcoming in explaining how to effectively use the product.

(b) (7)(E)

Attachment 2
U.S. Customs and Border Protection
Sole Source Determination
For actions above the micro-purchase threshold but not exceeding the SAT

3. The anticipated price will be determined fair and reasonable based on one or more of the price analysis techniques described below in accordance with FAR Part 13.106-3(a)(2). *(Check one and provide short explanation or description of action taken):*

_____Market Research.
_____Comparison of the proposed price with prices found reasonable on previous purchases.
_____Current price List.
_____x___Comparison with similar items in a related industry.
_____Comparison to IGCE.
_____Contracting Officer's personal knowledge.
_____Other. Explain:

Evidence that supporting data (*e.g.*, verification of the Government's minimum needs, requirements, or other rationale for limited sources) is complete and accurate.

(b) (7)(E) will continue to conduct cost comparison and product effectiveness with any similar products throughout the first year of the contract with Venntel. If any of the similar products meet Venntel's capabilities, and are cost effective, then (b) (7)(E) will reevaluate future acquisition of that product.

4. Technical/Requirements Personnel Certification:

I certify that this requirement meets the Government's minimum need and that the supporting data, which forms a basis for the Sole Source Determination, is accurate and complete.

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

Technical Representative/COR

9-1-20
Date

5. Contracting Officer Certification/Approval:

I hereby determine that the circumstances described herein exist and that the information is accurate and complete to the best of my knowledge:

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

Contracting Officer

9-1-20
Date

Attachment 2
U.S. Customs and Border Protection
Sole Source Determination
For actions above the micro-purchase threshold but not exceeding the SAT

ORDER FOR SUPPLIES OR SERVICES

CBP-2020-033428-0000552

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 BUS NESS (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) (4), (b) (7)(E)	(b) (7)(E), (b) (4)	
20			EA			
30	Venntel		EA	(b) (4), (b) (7)(E)		
40	Venntel - TASPD		EA			
50	Venntel (b)(7)(E) TASPD		EA			

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

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

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

OPTIONAL FORM 347 (REV. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213 (f)

DATEOF ORDER	CONTRACT NO. (if any)	ORDERNO.	PAGE OF PAGES
9/24/2019	HSHQDC-12-D-00013	70B04C19F00000802	2 4

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, 70B04C19F00000802, is issued against the Department of Homeland Security FirstSource II HSHQDC-12-D-00013 for (b)(7)(E) 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: (b)(6)(b)(7)(C)
Address: 5971 Kingstowne Village Pkwy.
5th floor mailroom
ndria, Virginia 22315
Tel. #: (b) (6), (b) (7)(C)
Fax. #:
Email: @cbp.dhs.gov

IPP APPROVER

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

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)	(b) (7)(E)	EA	(b) (4), (b) (7)(E)	(b) (7)(E), (b) (4)
20			EA		
30	Venntel		EA	(b) (4), (b) (7)(E)	
40	Venntel - TASPD		EA		
50	Venntel (b)(7)(E) 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)	(b) (7)(E), (b) (4)
20		
30	(b) (7)(E)	
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)	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]

(b) (7)(E)

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

LC Logon Instructions | Business Analytics - CBP Financ... | IPP

File Edit View Favorites Tools Help

Summary | My Tasks | My Queues | Task Delegations

Invoice Number: 208696

My Tasks | My Admin Tasks | Summary

Details
- Task Description: APPROVE:LEVEL 1 assigned to you on Oct 4, 2019 4:12 PM
- Task Instructions: Please review and approve this invoice.
- SAM Activation Status: Active (Oct 6, 2019 11:39 AM)

APPROVE | Re-Assign | Reject | View Current Attachments | Add Attachment

PANAMERICA COMPUTERS INC.

Remit To:
PANAMERICA COMPUTERS, INC. - 1027756
Panamerica Computers Inc.
1386 BIG OAK RD.
LURAY VA 22835
XMVL DUNS:166669742
XMVL DUNS+4:0000

Customs and Border Protection

ALC Code: 71050800

Bill To:
Customs and Border Protection

Is this the Final Invoice for this PO (Y/N Only) : Y

Business Unit: | Cost Center: 2N | Dept. ID:

Invoice Number:	208696
Issue Date:	Oct 4, 2019
Receipt Date:	Oct 4, 2019
Bill Period Start Date:	Sep 30, 2019
Bill Period End Date:	Oct 30, 2019
Supplier Contact Name:	(b) (6)
Supplier Contact Phone:	
Payment Terms:	Pay within 30 Days Due Net 30
Anticipated Due Date:	Nov 3, 2019
Prompt Pay Penalty:	0 day(s)
PO Number:	70[illegible]0000002 R 0
Contract No.:	[illegible]0001
Buyer Contact Name:	(b) (6), (b) (7)(C)
Buyer Phone:	
Buyer Email:	(b) (6), (b) (7)(C)@cbp.dhs.gov
COR:	(b) (6), (b) (7)(C)
COR Phone:	
COR Email:	
FOB Terms:	
Goods/Services Received Date:	
Goods/Services Accepted Date:	
First Approver Date:	
Prompt Pay Special Handling:	
Currency Code:	USD
PO Freight Limit:	0.00
Invoice Amount:	1,968,317.18

INV Line # Dist #	PO Line #	PO Sch. #	PO Dist #	Agency Part #	Item Code	Description	Service Date From	Service Date To	QTY	Unit Price	U.O.M. (Type)	Extended Price	Tax Type	Tax %	Tax Amount
1.1	10	1	1			(b) (7)(E)			(b) (7)(E)	(b) (7)(E), (b) (4)	Each (G)	(b) (7)(E), (b) (4)	Exempt	0.00	0.00
2.1	20	1	1								Each (G)		Exempt	0.00	0.00
3.1	30	1	1			Venntel					Each (G)		Exempt	0.00	0.00
4.1	40	1	1			Venntel - TASPD					Each (G)		Exempt	0.00	0.00
5.1	50	1	1			Venntel (b) (7)(E)					Each (G)		Exempt	0.00	0.00

Showing 1-5 of 5

Extended Price Sub-total:	1,968,317.18
Total Misc:	0.00
Total Freight:	0.00
Total Taxes:	0.00
(Totals apply to full invoice) Total Amount:	1,968,317.18

Invoice Comments:

100%

List Edit Goto Environment System Help

Purchasing Documents by Document Number

Print Preview | PO History | Changes | Delivery Schedule | Services

PO	Type	Vendor	Name			PGp	Order Date
Item	Material		Short Text				Mat. Group
D I A	Plnt	SLoc	Order Qty	Un	Net Price	Curr.	per Un
04C19F0802	ZDO	1027756	PANAMERICA COMPUTERS, INC.			YIT	09/24/2019
00010			(b) (7)(E)		(b) (7)(E), (b) (4)		315B
K	USCS			EA		USD	1 EA
Still to be delivered				EA		USD	100.00 %
Still to be invoiced				EA		USD	100.00 %
00020							315B
K	USCS			EA		USD	1 EA
Still to be delivered				EA		USD	100.00 %
Still to be invoiced				EA		USD	100.00 %
00030			Venntel		(b) (7)(E), (b) (4)		315B
K	USCS			EA		USD	1 EA
Still to be delivered				EA		USD	100.00 %
Still to be invoiced				EA		USD	100.00 %
00040			Venntel - TASPD				315B
K	USCS			EA		USD	1 EA
Still to be delivered				EA		USD	100.00 %
Still to be invoiced				EA		USD	100.00 %
00050			Venntel (b) (7)(E) - TASPD				315B
K	USCS			EA	(b) (7)(E), (b) (4)	USD	1 EA
Still to be delivered				EA		USD	100.00 %
Still to be invoiced				EA		USD	100.00 %

Page of Pages

DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection

REQUEST FOR PROPERTY OR SERVICES

Customs Directive 5220-26A

FOR USE BY PROCUREMENT STAFF	
Date Assigned	P.R. No. Assigned
Assigned to:	
Order No.	Award Amount $
Completion Date	Contract Specialist Telephone No.
Contract Specialist (Signature)	

Prepare in quadruplicate. Original and two copies to procurement office. Retain last copy for your records.

APPROVALS (Printed Name & Signature)

1. Organization Approval
OFO/NTC/CND

4. Funding Approval (Authorized Signature Only)
[redacted]

7a. Accounting Process Code (APC)

7b. Project Code

9a. Technology & Architecture Group Approval

9b. Non-IT Review Board Approval

10. Local Property Officer Approval

INITIATOR

2. Originator's Request No.

3. Request Date
04/01/2020

5. Requestor's Name
[redacted]

6. Telephone Number

8. Organization

Name OFO-NATIONAL TARGETING CENTER-CND

Address 22330 GLENN DRIVE

Room No.

City STERLING State VA Zip 20164

11. Item No.	12. Quantity	13. Unit of Measure	14. Object Class Code	15. Property Code	16. Property Location Code	17. Description	18. Estimated Cost A. Unit	18. Estimated Cost B. Total
1	[redacted]	$				Venntel	[redacted]	[redacted]

19. DELIVER TO (If other than blocks 5 and 8 above. Note that the accountable property location code must always be listed in column 16 above.)

20. Date Required
09/25/2020

21. Total Estimated Cost
[redacted]

22. Remarks:

23. Attachments Checklist

- ☐ Basic Justification (If not given in block 22 above)
- ☐ Physical and/or Performance Specifications
- ☐ Acceptance Tests
- ☐ Statement of Work
- ☐ Sole Source Justification
- ☐ Recommended Sources
- ☐ Statement of Urgency
- ☐ Other (describe)

DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection

REQUEST FOR PROPERTY OR SERVICES - CONTINUATION SHEET

Customs Directive 5220-26A

FOR USE BY PROCUREMENT STAFF	
Date Assigned	P.R. No. Assigned
Assigned to	
INITIATOR	
2. Originator's Request No.	3. Request Date 04/01/2020

11. Item No.	12. Quantity	13. Unit of Measure	14. Object Class Code	15. Property Code	16. Property Location Code	17. Description	18. Estimated Cost	
							A. Unit	B. Total

CBP Form 148 (03/07)

Add continuation page

Go to continuation page

CBP-2020-033428-0000560

DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection

REQUEST FOR PROPERTY OR SERVICES - CONTINUATION SHEET

Customs Directive 5220-26A

FOR USE BY PROCUREMENT STAFF	
Date Assigned	P.R. No. Assigned
Assigned to	

INITIATOR	
2. Originator's Request No.	3. Request Date 04/01/2020

11. Item No.	12. Quantity	13. Unit of Measure	14. Object Class Code	15. Property Code	16. Property Location Code	17. Description	18. Estimated Cost	
							A. Unit	B. Total

CBP Form 148 (03/07)

Add continuation page

Go to continuation page

CBP-2020-033428-0000561

DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection

REQUEST FOR PROPERTY OR SERVICES - CONTINUATION SHEET

Customs Directive 5220-26A

FOR USE BY PROCUREMENT STAFF	
Date Assigned	P.R. No. Assigned
Assigned to	
INITIATOR	
2. Originator's Request No.	3. Request Date 04/01/2020

11. Item No.	12. Quantity	13. Unit of Measure	14. Object Class Code	15. Property Code	16. Property Location Code	17. Description	18. Estimated Cost	
							A. Unit	B. Total

CBP Form 148 (03/07)

Add continuation page

Go to continuation page

CBP-2020-033428-0000562

DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection

REQUEST FOR PROPERTY OR SERVICES - CONTINUATION SHEET

Customs Directive 5220-26A

FOR USE BY PROCUREMENT STAFF	
Date Assigned	P.R. No. Assigned
Assigned to	

INITIATOR	
2. Originator's Request No.	3. Request Date 04/01/2020

11. Item No.	12. Quantity	13. Unit of Measure	14. Object Class Code	15. Property Code	16. Property Location Code	17. Description	18. Estimated Cost	
							A. Unit	B. Total

CBP Form 148 (03/07)

Add continuation page

Go to continuation page

[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]

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] (b)(6) (b)(7)(C)
Address: 5971 Kingstowne Village Pkwy.
5th floor mailroom
Alexandria, Virginia 22315
Tel. #: [redacted] (b) (6), (b) (7)(C)
Fax. #:
Email: [redacted]@cbp.dhs.gov

IPP APPROVER
Name: [redacted] (b)(6) (b)(7)(C)
Address: 5971 Kingstowne Village Pkwy.
5th floor mailroom
Alexandria, VA 22315
Tel. #: [redacted] (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).

DHS Enterprise Architecture Compliance

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.

Instructions to Offerors

1. For each commercially available Information and Communications Technology (ICT) item offered through this contract, the Offeror shall provide an Accessibility Conformance Report (ACR). The ACR shall be created using the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed in accordance with all the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Supports", "Supports with Exceptions", "Does Not Support", and "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. The offeror is cautioned to address each standard individually and with specificity, and to be clear whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. The ACR shall provide a description of the evaluation methods used to support Section 508 conformance claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror's proposed ICT items to validate Section 508 conformance claims made in the ACR.

2. For each commercially available authoring tool offered that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the Offeror shall describe the level of Section 508 compliance supported for the content that can be generated.

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.

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 th (b) (7)(E) [redacted] 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) [redacted] *In accordance with the attached Bill of Materials	(b) (7)(E) [redacted]
(b) (7)(E) [redacted] *In accordance with the attached Bill of Materials	
(b) (7)(E) [redacted] *In accordance with the attached Bill of Materials	
Venntel *In accordance with the attached Bill of Materials	(b)(7)(E) [redacted]

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 12 months from the Date of Award.

1.2 PLACE OF PERFORMANCE

Place of performance will be at government facilities.

2.0 SPECIFIC TASKS

2. (b) (7)(E)

(b) (7)(E)

2. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

2. (b) (7)(E)

(b) (7)(E)

2.4 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.

Under this contract, the following documents are required to be submitted as an attachment to the IPP invoice [CO to edit and include the documentation required under this contract]:

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] (b)(6) (b)(7)(C)
Address: 5971 Kingstowne Village Pkwy.
5th floor mailroom
Alexandria, Virginia 22315
Tel. #: [redacted] (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).

DHS Enterprise Architecture Compliance

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.