ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 2

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

1. DATE OF ORDER: 09/07/2021
2. CONTRACT NO. (if any): HSHQDC12D00013
3. ORDER NO.: 70B03C21F00001121
4. REQUISITION/REFERENCE NO.: 0020125925
5. ISSUING OFFICE (Address correspondence to):
DHS - Customs & Border Protection
Border Enforcement Contracting Division
Intech Two, Suite 100
6650 Telecom Drive
Indianapolis IN 46278

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: DBA PCI TEC
c. STREET ADDRESS: 1386 BIG OAK RD
d. CITY: LURAY
e. STATE: VA
f. ZIP CODE: 22835-5233

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

9. ACCOUNTING AND APPROPRIATION DATA:

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

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

12. F.O.B. POINT: Destination

13. PLACE OF
a. INSPECTION
b. ACCEPTANCE

14. GOVERNMENT B/L NO.:

15. DELIVER TO F.O.B POINT ON OR BEFORE (Date): 09/22/2021

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	Babel BX/LXP Equipment				(b) (4)	

18. SHIPPING POINT:
19. GROSS SHIPPING WEIGHT:
20. INVOICE NO.:
(b) (4)
17(h) TOT. (Cont. pages)

SEE BILLING INSTRUCTIONS REVERSE

21. MAIL INVOICE TO:
a. NAME: See IPP Invoicing Instructions
b. STREET ADDRESS (or P.O. Box):
c. CITY:
d. STATE:
e. ZIP CODE:

$3,799,814.18
17(i) GRAND TOTAL

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

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

DATE OF ORDER	CONTRACT NO. (if any)	ORDER NO.	PAGE OF PAGES
09/07/2021	HSHQDC12D00013	70B03C21F00001121	2 2

Federal Tax Exempt ID: 72-0408780

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

NOTES:

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

ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: 70B03C21F00001121

I.1 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	Babel BX/LXP Equipment	(b) (4)			

Total Funded Value of Award: **$3,799,814.18**

I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.315BUSCSGLCS0936190700Z00021500TT0600000000 69600315B TAS# 07020212021 0530000	(b) (4)

I.3 DELIVERY SCHEDULE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
(b) (6), (b) (7)(C)	(b) (4)		09/22/2021

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 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of (DEVIATION) after the date of the clause.

(b) The use in this solicitation or contract of any HSAM clause with an authorized deviation is indicated by the addition of (DEVIATION) after the name of the regulation.

(End of clause)

I.6 52.204-23 - PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (DEVIATION 20-05)

(a) Definitions. As used in this clause --

"*Covered article*" means any hardware, software, or service that –

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

"*Covered entity*" means --

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from --

(1) Providing any covered article that the Government will use on or after October 1, 2018; and

(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) *Reporting requirement*.

(1) In the event the Contractor identifies covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report, in writing, via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at NDAA_Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Page 5 of 8 Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

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

(i) Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(c) *Subcontracts*. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

I.7 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (DEVIATION 20-05) (DEC 2020)

(a) *Definitions*. As used in this clause --

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

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

"*Covered telecommunications equipment or services*" means --

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

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

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

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

"*Critical technology*" means --

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

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

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

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

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

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

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

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

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

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

"*Roaming*" means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

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

(b) *Prohibition*.

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

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

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

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

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

(d) *Reporting requirement*.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer's Representative, and the Network Operations Security Center (NOSC) at NDAA_Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the NOSC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

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

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

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

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

(End of clause)

I.8 52.219-3 NOTICE OF HUBZONE SET-ASIDE OR SOLE SOURCE AWARD (DEVIATION 19-01) (AUG 2020)

(a) *Definition.* "*HUBZone small business concern*," as used in this clause, means a small business concern, certified by the Small Business Administration (SBA), that appears on the List of Qualified HUBZone Small Business Concerns maintained by the SBA (13 CFR 126.103).

(b) *Applicability*. This clause applies only to --

(1) Contracts that have been set aside or awarded on a sole source basis to, HUBZone small business concerns;

(2) Part or parts of a multiple-award contract that have been set aside for HUBZone small business concerns;

(3) Orders set aside for HUBZone small business concerns under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F); and

(4) Orders issued directly to HUBZone small business concerns under multiple-award contracts as described in 19.504(c)(1)(ii).

(c) *General*.

(1) Offers are solicited only from HUBZone small business concerns. Offers received from concerns that are not HUBZone small business concerns will not be considered.

(2) Any award resulting from this solicitation will be made to a HUBZone small business concern.

(d) *Notice*. The HUBZone small business offeror acknowledges that a prospective HUBZone awardee must be a HUBZone small business concern at the time of award of this contract. The HUBZone offeror shall provide the Contracting Officer a copy of the notice required by 13 CFR 126.501 if material changes occur before contract award that could affect its HUBZone eligibility. If the apparently successful HUBZone offeror is not a HUBZone small business concern at the time of award of this contract, the Contracting Officer will proceed to award to the next otherwise successful HUBZone small business concern or other offeror.

(End of clause)

I.9 52.219-4 NOTICE OF PRICE EVALUATION PREFERENCE FOR HUBZONE SMALL BUSINESS CONCERNS (DEVIATION 19-01) (AUG 2020)

(a) *Evaluation preference*.

(1) Offers will be evaluated by adding a factor of 10 percent to the price of all offers, except --

(i) Offers from HUBZone small business concerns that have not waived the evaluation preference; and

(ii) Otherwise successful offers from small business concerns.

(2) The factor of 10 percent shall be applied on a line item basis or to any group of items on which award may be made. Other evaluation factors described in the solicitation shall be applied before application of the factor.

(3) When the two highest rated offerors are a HUBZone small business concern and a large business, and the evaluated offer of the HUBZone small business concern is equal to the evaluated offer of the large business after considering the price evaluation preference, award will be made to the HUBZone small business concern.

(b) *Waiver of evaluation preference*. A HUBZone small business concern may elect to waive the evaluation preference, in which case the factor will be added to its offer for evaluation purposes.

[_] Offeror elects to waive the evaluation preference.

(c) *Notice*. The HUBZone small business offeror acknowledges that a prospective HUBZone awardee must be a HUBZone small business concern at the time of award of this contract. The HUBZone offeror shall provide the Contracting Officer a copy of the notice required by 13 CFR 126.501 if material changes occur before contract award that could affect its HUBZone eligibility. If the apparently successful HUBZone offeror is not a HUBZone small business concern at the time of award of this contract, the Contracting Officer will proceed to award to the next otherwise successful HUBZone small business concern or other offeror.

(End of clause)

I.10 52.219-14 LIMITATIONS ON SUBCONTRACTING (DEVIATION 19-01) (AUG 2020)

(a) This clause does not apply to the unrestricted portion of a partial set-aside.

(b) *Definition*. "*Similarly situated entity*," as used in this clause, means a first-tier subcontractor, including an independent contractor, that--

(1) Has the same small business program status as that which qualified the prime contractor for the award (e.g., for a small business set-aside contract, any small business concern, without regard to its socioeconomic status); and

(2). Is considered small for the size standard under the North American Industry Classification System (NAICS) code the prime contractor assigned to the subcontract.

(c) Applicability. This clause applies only to--

(1) Contracts that have been set aside for any of the small business concerns identified in 19.000(a)(3);

(2) Part or parts of a multiple-award contract that have been set aside for any of the small business concerns identified in 19.000(a)(3);

(3) Contracts that have been awarded on a sole-source basis in accordance with subparts 19.8, 19.13, 19.14, and 19.15;

(4) Orders expected to exceed the simplified acquisition threshold and that are--

(i) Set aside for small business concerns under multiple-award contracts, as described in 8.405-5 and 16.505(b)(2)(i)(F);or

(ii) Issued directly to small business concerns under multiple-award contracts as described in 19.504(c)(1)(ii);

(5) Orders, regardless of dollar value, that are--

(i) Set aside in accordance with subparts 19.8, 19.13, 19.14, or 19.15 under multiple-award contracts, as described in 8.405-5 and 16.505(b)(2)(i)(F); or

(ii) Issued directly to concerns that qualify for the programs described in subparts 19.8, 19.13, 19.14, or 19.15 under multiple-award contracts, as described in 19.504(c)(1)(ii); and

(6) Contracts using the HUBZone price evaluation preference to award to a HUBZone small business concern unless the concern waived the evaluation preference.

(d) Independent contractors. An independent contractor shall be considered a subcontractor.

(e) Limitations on subcontracting. By submission of an offer and execution of a contract, the Contractor agrees that, in performance of a contract assigned a North American Industry Classification System (NAICS) code for--

(1) Services (except construction), it will not pay more than 50 percent of the amount paid by the Government for contract performance to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 50 percent subcontract amount that cannot be exceeded. When a contract includes both services and supplies, the 50 percent limitation shall apply only to the service portion of the contract;

(2) Supplies (other than procurement from a non- manufacturer of such supplies), it will not pay more than 50 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 50 percent subcontract amount that cannot be exceeded. When a contract includes both supplies and services, the 50 percent limitation shall apply only to the supply portion of the contract;

(3) General construction, it will not pay more than 85 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 85 percent subcontract amount that cannot be exceeded; or

(4) Construction by special trade contractors, it will not pay more than 75 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 75 percent subcontract amount that cannot be exceeded.

(f) The Contractor shall comply with the limitations on subcontracting as follows:

(1) For contracts, in accordance with paragraphs (c)(1), (2), (3), and (6) of this clause –

Contracting Officer check as appropriate.

[] By the end of the base term of the contract and then by the end of each subsequent option period; or

[] By the end of the performance period for each order issued under the contract.

(2) For orders, in accordance with paragraphs (c)(4) and (5) of this clause, by the end of the performance period for the order.

(g) A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (e) of this clause will be performed by the aggregate of the joint venture participants.

(End of clause)

I.11 52.222-19 CHILD LABOR -- COOPERATION WITH AUTHORITIES AND REMEDIES (DEVIATION 20-07)

(a) *Applicability.* This clause does not apply to the extent that the Contractor is supplying end products mined, produced, or manufactured in --

(1) Israel, and the anticipated value of the acquisition is $50,000 or more;

(2) Mexico, and the anticipated value of the acquisition is $83,099 or more; or

(3) Armenia, Aruba, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, Italy, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Singapore, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Taiwan, Ukraine, or the United Kingdom and the anticipated value of the acquisition is $182,000 or more.

(b) *Cooperation with Authorities.* To enforce the laws prohibiting the manufacture or importation of products mined, produced, or manufactured by forced or indentured child labor, authorized officials may need to conduct investigations

to determine whether forced or indentured child labor was used to mine, produce, or manufacture any product furnished under this contract. If the solicitation includes the provision 52.222-18, Certification Regarding Knowledge of Child Labor for Listed End Products, or the equivalent at 52.212-3(i), the Contractor agrees to cooperate fully with authorized officials of the contracting agency, the Department of the Treasury, or the Department of Justice by providing reasonable access to records, documents, persons, or premises upon reasonable request by the authorized officials.

(c) *Violations*. The Government may impose remedies set forth in paragraph (d) for the following violations:

(1) The Contractor has submitted a false certification regarding knowledge of the use of forced or indentured child labor for listed end products.

(2) The Contractor has failed to cooperate, if required, in accordance with paragraph (b) of this clause, with an investigation of the use of forced or indentured child labor by an Inspector General, Attorney General, or the Secretary of the Treasury.

(3) The Contractor uses forced or indentured child labor in its mining, production, or manufacturing processes.

(4) The Contractor has furnished under the contract end products or components that have been mined, produced, or manufactured wholly or in part by forced or indentured child labor. (The Government will not pursue remedies at paragraph (d)(2) or paragraph (d)(3) of this clause unless sufficient evidence indicates that the Contractor knew of the violation.)

(d) *Remedies*.

(1) The Contracting Officer may terminate the contract.

(2) The suspending official may suspend the Contractor in accordance with procedures in FAR Subpart 9.4.

(3) The debarring official may debar the Contractor for a period not to exceed 3 years in accordance with the procedures in FAR Subpart 9.4.

(End of clause)

I.12 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013) (DEVIATION APR 2020)

(a) (1) In accordance with 31 U.S.C. 3903 and 10 U.S.C. 2307, upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract in accordance with the accelerated payment date established, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, with a goal of 15 days after receipt of a proper invoice and all other required documentation from the small business subcontractor if a specific payment date is not established by contract.

(2) The Contractor agrees to make such payments to its small business subcontractors without any further consideration from or fees charged to the subcontractor.

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

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

(End of clause)

I.13 CONTRACT TYPE (OCT 2008)

This is a Firm FIxed Price Delivery Order.

[End of Clause]

I.14 PERIOD OF PERFORMANCE (MAR 2003)

The period of performance of this contract shall be from 09/22/2021 through 09/21/2022.

[End of Clause]

I.15 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.16 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*:*

Invoices

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.17 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

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

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

[End of Clause]

I.18 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct

background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:

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

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

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

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

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

[End of Clause]

PRIVACY THRESHOLD ANALYSIS (PTA)

This form will be used to determine whether a Privacy Impact Assessment (PIA), System of Records Notice (SORN), or other privacy compliance documentation is required under the E-Government Act of 2002, the Homeland Security Act of 2002, the Privacy Act of 1974, or DHS policy.

Please complete this form and send it to your Component Privacy Office. If you are unsure of your Component Privacy Office contact information, please visit https://www.dhs.gov/privacy-office-contacts. If you do not have a Component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
DHS Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717

PIA@hq.dhs.gov

Your Component Privacy Office will submit the PTA on behalf of your office. Upon receipt from your Component Privacy Office, the DHS Privacy Office will review this form. If a PIA, SORN, or other privacy compliance documentation is required, your Component Privacy Office, in consultation with the DHS Privacy Office, will send you a copy of the template to complete and return.

For more information about the DHS Privacy compliance process, please see https://www.dhs.gov/compliance. A copy of the template is available on DHS Connect at http://dhsconnect.dhs.gov/org/offices/priv/Pages/Privacy-Compliance.aspx or directly from the DHS Privacy Office via email: PIA@hq.dhs.gov or phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project, Program, or System Name:	Babel Street "BabelX" Platform		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	OFO
FISMA Name (if applicable):	Click here to enter text.	**FISMA Number (if applicable):**	Click here to enter text.
Type of Project or Program:	**Pilot**	**Project or program status:**	**Operational**
Date first developed:	**January 1, 2018**	**Pilot launch date:**	**September 26, 2019**
Date of last PTA update		**Pilot end date:**	**September 25, 2023**
ATO Status (if applicable):[1]	**Not started**	**Expected ATO/ATP/OA date (if applicable):**	Click here to enter a date.

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b)(6) (b)(7)(C)		
Office:	**OFO**	**Title:**	(A) Director
Phone:	Click here to enter text.	**Email:**	SCOTT.P.FOSTER@CBP.DHS.GOV

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Click here to enter text.		
Phone:	Click here to enter text.	**Email:**	Click here to enter text.

[1] The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/CISO%20ALL%20Documents/Authority%20to%20Proceed%20Memo%20Phase%20II.pdf.

Specific PTA Questions

1. Reason for submitting the PTA: New PTA

Background

(U//LES) U.S. Customs and Border Protection (CBP), Office of Field Operations (OFO), National Targeting Center (NTC), Counter Network Division (CND), Publicly Available Information Group (PAIG) is submitting this PTA to continue to pilot the use of Babel Street's BabelX platform. BabelX provides CBP with advanced capabilities in several areas of Publicly Available Information (PAI) and social media research which assist in mission critical CBP operations. The product is a multi-lingual, geo-enabled, text-analytics, social media and web-monitoring platform designed to meet the needs of its customers by fully leveraging PAI.

(U//LES) Babel X is an open source, intelligence monitoring web-based platform designed specifically to meet the needs of the Intelligence Community (IC) and federal law enforcement in developing Open Source Intelligence (OSINT). The platform can search for keywords and keyword combinations, phrases, hash tags, and names. It can handle requests across more than 52+ social media platforms and millions of URLs and deep/dark web data. Babel X can perform cross-lingual searches across more than 200 languages, allowing users to enter terms in English and return foreign language results. The platform also has the ability to build sophisticated filtering options for catered feeds and render various data visualizations. Lastly, Babel X allows for networks discovery with social media link analysis and provides user anonymity in viewing collected results.

(U//LES) Users can create hotlists based on events or known terms used by bad actors in order to identify derogatory information or information that may show threats to CBP and national security. A BabelX user will then review any hits to determine if information is relevant and should be retained.

(U//LES) BabelX makes sense of large tracts of multi-lingual data in near real time. Users identify themes, entities, and categories, as well as detect relationships, within the cloud based platform. Babel users can explore the data through a wide range of analytical lenses to include geospatial, temporal, link analysis, public records search, sentiment, and topics of interest.

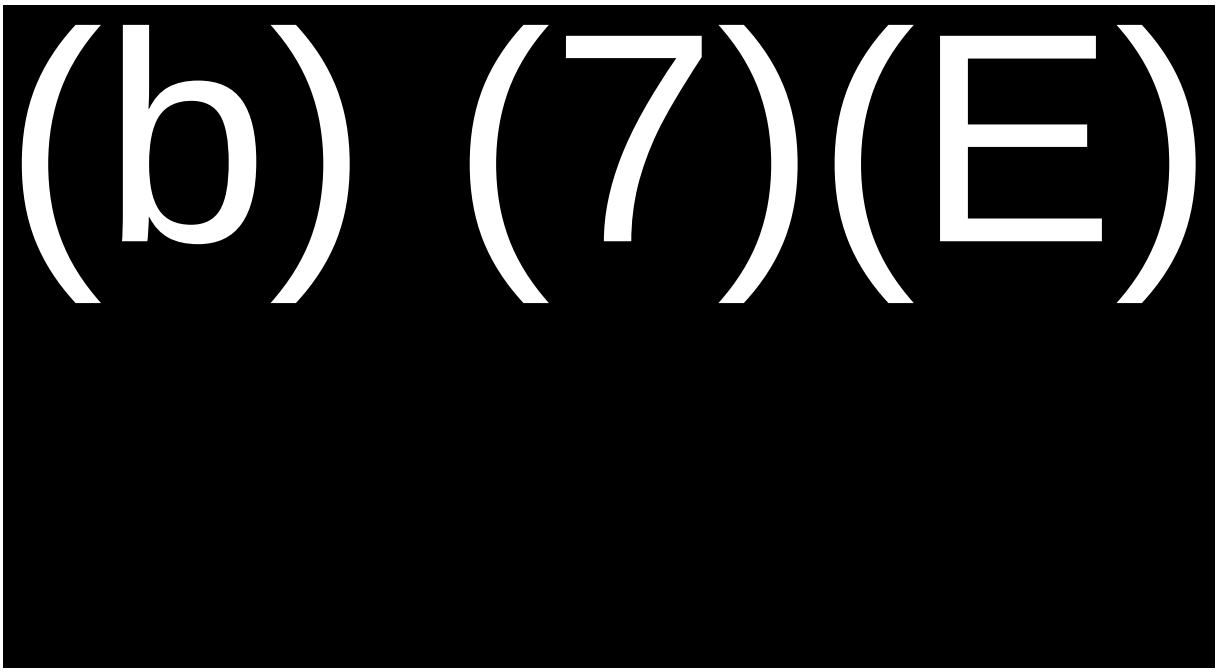
- Built in translation of searches and search results in a wide variety of applicable languages, with a built in ontology capability;
- Easy customization and incorporation of new publically available data sets;
- Public records database capabilities;
- Powerful search capability for law enforcement targets; and

(U//LES) BabelX has the ability to create geofences so CBP can view information posted from or about certain locations only. (b) (7)(E) (b) (7)(E) BabelX knows location information if

individual's have geolocation turned on for their posts. This PTA covers BabelX and not LocateX which uses AdID information to determine location. LocateX is covered by the commercial telemetry PTA.

(U//FOUO//LES) Enhancing CBP's Targeting Enterprise

Babel data will be used/captured/stored in support of CBP targeting, vetting, operations and analysis. This will parallel already existing CBP efforts to leverage PAI. During this pilot, activities will be fluid to allow research on a range of activities and will be used to identify potential derogatory and confirmatory information associated with traveler's, persons seeking benefits, and persons of interest. CBP does no rely solely on information found in BabelX when taking actions. Relevant information would be retained as follows:



(U// LES) CBP will not retain PII unless the information is put into one of the above systems and linked to an individual as derogatory or to confirm information.

(U// LES) For technical help, 3 Babel Street employees have access to CBP queries, but only upon request from CBP and in an audited and access restricted "vault." BabelX stores queries forever, however it does not store results of queries.

2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This project does not collect, store, maintain, use, or disseminate any personally identifiable information[2] ☒ Members of the public ☒ U.S. Persons (U.S citizens or lawful permanent residents) ☒ Non-U.S. Persons ☐ DHS Employees/Contractors (list Components): *Click here to enter text.* ☐ Other federal employees or contractors (list agencies): *Click here to enter text.*
2(a) Is information meant to be collected from or about sensitive/protected populations?	☐ No ☐ 8 USC § 1367 protected individuals (e.g., T, U, VAWA)[3] ☒ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

3. What specific information about individuals is collected, maintained, used, or disseminated?

Please provide a specific description of information that is collected, generated, or retained (such as names, addresses, emails, etc.) for each category of individual or population.

(U//LES) Babel may assist analysts with locating and assessing the following publicly available information:

First, Middle, Last Name
Date of Birth
Address

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

[3] This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, *available at* http://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/002-02.pdf.

Usernames Email Address Phone Number Social Media Content Images IP Address Domain Information Social Security Number Driver's License Number Employment History Location data based on geolocation tags in public posts AdID information is available through locateX

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?[4] If applicable, check all that apply.

Social Security number ☐ Alien Number (A-Number) ☐ Tax Identification Number ☐ Visa Number ☐ Passport Number ☐ Bank Account, Credit Card, or other financial account number Driver's License/State ID Number	Social Media Handle/ID ☐ Biometric identifiers *(e.g., FIN, EID)* ☐ Biometrics.[5] *Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text.* ☐ Other. *Please list: Click here to enter text.*

3(b) Please provide the specific legal basis for the collection of SSN:	(U//FOUO) CBP is proposing to obtain access to commercially available records, some of which contain social security numbers compiled by private third parties. CBP is not proposing to collect SSNs directly from individuals as part of this effort. CBP obtains access to commercially available information in furtherance of its statutory law enforcement and border security responsibilities. See, e.g., 6 U.S.C. 211; The Tariff Act of 1930, as

[4] Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

[5] If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS' IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.

	amended; The Immigration and Nationality Act ("INA"), as amended, 8 U.S.C. § 1101, et seq
3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.	
(U//LES) SSN is not "required" to conduct queries to fulfill the requirement of the platform. CBP will conduct social security number queries on a case by case basis and will be utilized like other selectors of interest (when available or identified through other queries). Through Babel's partnership agreements with public and private data sources, it is able to combine PAI with identifiers such as SSNs. (U//LES) CBP is primarily using Babel data to lookup telephone numbers, email addresses, usernames in order to develop confirmatory or derogatory information. On occasion, when a telephone number is queried, an individual's name, address and SSN, among others, will be returned as a result.	
3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, *SSN Collection and Use Reduction*,[6] which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: *even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.*	
(U//FOUO) SSN is not "required" to conduct queries to fulfill the requirement of the platform. CBP will conduct social security number queries on a case by case basis and will be utilized like other selectors of interest (when available or identified through other queries).	

4. How does the Project, Program, or System retrieve information?	☒ By a unique identifier.[7] Please list all unique identifiers used: Same as above in #3. (U//LES) Username, Email, Name, Street Address, City, State, Zip Code, Country, Social Security Number, Driver's License Number, Domain Name, IP Address, telephone number ☒ By a non-unique identifier or other means. Please describe:

[6] *See* https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction.
[7] Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S , or employee or contractor to the Department.

	(U//LES) BabelX users can create geofences for publicly available geotagged social media content.

5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)? *If no schedule has been approved, please provide proposed schedule or plans to determine it.* *Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.*[8]	(U//FOUO) For queries conducted in BabelX, those queries will be stored within Babel forever. The results of those queries are not saved or retained by the vendor. Access to individual account search queries is accessed/maintained by the vendors Director of Technology for auditing purposes. The vendor is currently creating an Administrator Module where an assigned CBP administrator will be able to review individual queries conducted by any CBP user for auditing purposes. The results/findings/analysis of queries conducted by CBP operators and analysts will be maintained in approved CBP Systems of Record such as Automated Targeting System (ATS), Analytical Framework for Intelligence (AFI), Intelligence Reporting System –Next Generation (IRS-NG), and/or TECS for 75 years.
5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)**?**	(U//FOUO) For queries conducted in BabelX, those queries will be stored within BabelX forever. The results of those queries are not saved or retained by the vendor. Access to individual account search queries is accessed/maintained by the vendor's Director of Technology for auditing purposes. CBP program manager gets monthly reports from the Vendor on usage statistics and can request audit logs for any CBP accounts as appropriate for auditing purposes. The results/findings/analysis of queries conducted by CBP operators and analysts will be maintained in approved CBP Systems of Record.

6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?[9]	☒ No. ☐ Yes. If yes, please list:

[8] *See* http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/IS2O/rm/Pages/RIM-Contacts.aspx
[9] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in IACS.

7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?	☐ No. ☒ Yes. If yes, please list: This is a commercial entity that shares with other U.S. government agencies.
8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? *If applicable, please provide agreement as an attachment.*	Choose an item. Please describe applicable information sharing governance in place: *Click here to enter text.*
9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?	☒ No. What steps will be taken to develop and maintain the accounting: *Click here to enter text.* ☐ Yes. In what format is the accounting maintained: *Click here to enter text.*

10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	☒ Social Media ☐ Advanced analytics[10] ☐ Live PII data for testing ☐ No

[10] The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.

11. Does this Project, Program, or System use data to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)?[11] This does not include subject-based searches.	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*
11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*

12. Does the planned effort include any interaction or intervention with human subjects[12] via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes	☒ No. ☐ Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for independent review and approval of this effort.[13]

13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, in addition to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: CBP personnel using the database are required to act in accordance with CBP's existing authorities and in compliance with the CBP Social Media Directive (including completing the required training) and Social Media Rules of Behavior.

[11] Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—
(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;
(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and
(C) the purpose of the queries, searches, or other analyses is not solely—
(i) the detection of fraud, waste, or abuse in a Government agency or program; or
(ii) the security of a Government computer system.

[12] Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

[13] For more information about CAPO and their points of contact, please see: https://www.dhs.gov/publication/compliance-assurance-program-office or https://collaborate.st.dhs.gov/orgs/STCSSites/SitePages/Home.aspx?orgid=36. For more information about the protection of human subjects, please see DHS Directive 026-04: https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir_026-04-protection-of-human-subjects_revision-01.pdf.

14. Is there a FIPS 199 determination?[14]	☒ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6) (b)(7)(C)
Date submitted to Component Privacy Office:	*Click here to enter a date.*
Concurrence from other Component Reviewers involved (if applicable):	*Click here to enter text.*
Date submitted to DHS Privacy Office:	*November 17, 2020*

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.

(b) (5)

[14] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

(b) (5)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6) (b)(7)(C)
DHS Privacy Office Approver (if applicable):	*Click here to enter a date.*
Workflow Number:	*Click here to enter text.*
Date approved by DHS Privacy Office:	*December 14, 2020*
PTA Expiration Date	*September 25, 2023*

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	System If "other" is selected, please describe: *Click here to enter text.*
Determination:	☒ Project, Program, System in compliance with full coverage ☐ Project, Program, System in compliance with interim coverage ☐ Project, Program, System in compliance until changes implemented ☐ Project, Program, System not in compliance
PIA:	**System covered by existing PIA** DHS/CBP/PIA-058 Publicly Available Social Media Monitoring and Situational Awareness Initiative; DHS/CBP/PIA-007 ESTA; DHS/CBP/PIA-009 TECS; DHS/CBP/PIA-006 ATS; Forthcoming IRS-NG and Trusted Traveler Programs PIAs
SORN:	System covered by existing SORN DHS/CBP-002 Trusted and Registered Traveler Programs, March 11, 2020, 85 FR 14214; DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297;

	DHS/CBP-009 Electronic System for Travel Authorization (ESTA); DHS/CBP-011 U.S. Customs and Border Protection TECS; DHS/CBP-024 Intelligence Records System (CIRS) System of Records

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.

(U//LES) CBP is submitting this PTA to discuss a pilot of Babel Street's BabelX platform, which is an open source, intelligence monitoring web-based platform that will provide CBP with advanced capabilities in several areas of Publicly Available Information (PAI) and social media research to assist in mission critical CBP operations.

(U//LES) The platform can perform cross-lingual searches (i.e., entering English search terms and returning foreign language results) for keywords and keyword combinations, phrases, hashtags, and names across 52+ social media platforms and millions of URLs and deep/dark web data. The platform can also build filtering options for catered feeds and render various data visualizations. Users can identify themes, entities, and categories, as well as detect relationships, and can explore the data through a wide range of analytical lenses such as geospatial, temporal, link analysis, public records search, sentiment, and topics of interest.

(b) (7)(E)

The DHS Privacy Office agrees this pilot is privacy sensitive and requires PIA coverage. As BabelX will be used for a variety of specific targeting and vetting operations and analysis, coverage is dependent on the specific use of the tool. Social media monitoring and situational awareness is covered by DHS/CBP/PIA-058 Publicly Available Social Media Monitoring and Situational Awareness Initiative. Coverage for various vetting and targeting activities is provided by DHS/CBP/PIA-007 Electronic System for Travel Authorization (ESTA), DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, DHS/CBP/PIA-006 Automated Targeting System (ATS), as well as the forthcoming IRS-NG and Trusted Traveler Program PIAs.

SORN coverage is also required and is provided by DHS/CBP-006 ATS, DHS/CBP-002 Trusted and Registered Traveler Programs, DHS/CBP-011 U.S. Customs and Border Protection TECS, DHS/CBP-009 Electronic System for Travel Authorization (ESTA), and DHS/CBP-024 Intelligence Records System (CIRS) System of Records.

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 8

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

1. DATE OF ORDER: 09/21/2017
2. CONTRACT NO. (if any): HSHQDC-13-D-00026
3. ORDER NO.: HSBP1017J00831
4. REQUISITION/REFERENCE NO.: 0020094963

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: THUNDERCAT TECHNOLOGY LLC
b. COMPANY NAME:
c. STREET ADDRESS: 1925 ISAAC NEWTON SQ STE 180
d. CITY: RESTON
e. STATE: VA
f. ZIP CODE: 20190-5030

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: SEE ATTACHED

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

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

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

13. PLACE OF: a. INSPECTION: b. ACCEPTANCE:
14. GOVERNMENT B/L NO.:
15. DELIVER TO F.O.B POINT ON OR BEFORE (Date): 09/20/2018
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	BabelX Software Subscription - Renewal				(b) (4)	
20	BabelX Software Subscription - NEW					
30	BabelX Software Subscription-Batch Upld					

18. SHIPPING POINT:
19. GROSS SHIPPING WEIGHT:
20. INVOICE NO.:
(b) (4)
17(h) TOT. (Cont. pages)

SEE BILLING INSTRUCTIONS REVERSE

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

$981,005.20
17(i) GRAND TOTAL

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

AUTHORIZED FOR LOCAL REPR... 2/2012)
PREVIOUS EDITION NOT USABL... 3.213 (f)

DATE OF ORDER	CONTRACT NO. (if any)	ORDER NO.	PAGE OF PAGES
09/21/2017	HSHQDC-13-D-00026	HSBP1017J00831	2 8

Federal Tax Exempt ID: 72-0408780

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

NOTES:

This firm-fixed-price delivery order, HSBP1017J00831, is issued against the DHS FirstSource II IDIQ Contract, HSHQDC-13-D-00026, for (b) (7)(E)

(b) (7)(E)

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

ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: HSBP1017J00831

I.1 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	BabelX Software Subscription - Renewal	(b) (4)			
20	BabelX Software Subscription - NEW				
30	BabelX Software Subscription-Batch Upld				

Total Funded Value of Award: **$981,005.20**

I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.315BUSCSGLCS0942715000Z00017500TT060000AE00 IU549315B TAS# 07020172017 0530000	(b) (4)
20	6100.315BUSCSGLCS0942715000Z00017500TT060000AE00 IU549315B TAS# 07020172017 0530000	
30	6100.315BUSCSGLCS0942715000Z00017500TT060000AC00 IU549315B TAS# 07020172017 0530000	

I.3 DELIVERY SCHEDULE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
(b) (7)(E)	(b) (4)		09/20/2018
			09/20/2018
			09/20/2018

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

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

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

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

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

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

(End of clause)

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

(a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment

is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

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

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

(End of clause)

I.6 52.203-19 PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)

I.7 52.209-10 PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS (NOV 2015)

I.8 3052.205-70 ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASES (SEP 2012) ALTERNATE I (SEP 2012)

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

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

(End of clause)

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

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

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

(1) Have access to a system of records;

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

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

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

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

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

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

(1) Have a system of records;

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

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

(End of clause)

I.10 PERIOD OF PERFORMANCE (MAR 2003)

The period of performance of this contract shall be from 09/21/2017 through 09/20/2018.

[End of Clause]

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

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

[End of Clause]

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

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

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

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

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

(End of Clause)

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

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

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

[End of Clause]

I.14 SECURITY PROCEDURES (OCT 2009)

A. Controls

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

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

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

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

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

6. The Contractor shall provide employee departure/separation date and reason for leaving to the CO/COTR in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the Contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

B. Security Background Investigation Requirements

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

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

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

4. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, place of birth (city and state), and date of birth of employee candidates who possess

favorably adjudicated BI or SSBI that meets federal investigation standards.. For employee candidates needing a BI for this contract, the Contractor shall require the applicable employees to submit information and documentation requested by CBP to initiate the BI process.

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

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

C. Security Responsibilities

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

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

3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.

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

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

D. Notification of Contractor Employee Changes

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

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

E. Non-Disclosure Agreements

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

[End of Clause]

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

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

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

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

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

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

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

[End of Clause]