ORDER FOR SUPPLIES OR SERVICES

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)

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

$981,005.20
17(i) GRAND TOTAL

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

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

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]