

# ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 5

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

1. DATE OF ORDER 08/16/2010	2. CONTRACT NO. (if any) HSHQDC07D00021	6. SHIP TO:		
3. ORDER NO. HSBP1010J00572		4. REQUISITION/REFERENCE NO. 0020053319		
5. ISSUING OFFICE (Address correspondence to) DHS - Customs & Border Protection CBP, Procurement Directorate Intech Two, Suite 100 6650 Telecom Drive Indianapolis IN 46278		a. NAME OF CONSIGNEE See Attached Delivery Schedule		
		b. STREET ADDRESS		
		c. CITY	d. STATE	e. ZIP CODE
		f. SHIP VIA		
7. TO:		8. TYPE OF ORDER		
a. NAME OF CONTRACTOR COMPUTER WORLD SERVICES CORP		<input type="checkbox"/> 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. COMPANY NAME		<input checked="" type="checkbox"/> 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.		
c. STREET ADDRESS 1100 G STREET NW, STE 625				
d. CITY WASHINGTON	e. STATE DC	f. ZIP CODE 20001		10. REQUISITIONING OFFICE <b>(b) (6)</b>
9. ACCOUNTING AND APPROPRIATION DATA		11. BUSINESS CLASSIFICATION (Check appropriate box(es))		
CONTRACTOR TIN: <b>(b)(3); (b)(4)</b>		<input checked="" type="checkbox"/> a. SMALL <input type="checkbox"/> b. OTHER THAN SMALL <input checked="" type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input checked="" type="checkbox"/> e. HUBZone <input type="checkbox"/> f. EMERGING SMALL BUSINESS <input type="checkbox"/> g. SERVICE-DISABLED VETERAN-OWNED		
12. F.O.B. POINT      Destination				
13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 09/30/2010	16. DISCOUNT TERMS Net 30
a. INSPECTION	b. ACCEPTANCE			

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Accept
10	<b>(b) (7)(E)</b> 13,000 - AFIL/N	1,000	AU		<b>(b) (4)</b>	
20	<b>(b) (7)(E)</b> 4,000 - AFIL/N	1,000	AU			
30	<b>(b) (7)(E)</b> 13,000 - AFIL/N	1,000	AU			
40	<b>(b) (7)(E)</b> 1000 hits/mo-AFIL/N	1,000	AU			
50	<b>(b) (7)(E)</b> 1000 hits/mo-AFIL/N	1,000	AU			
60	<b>(b) (7)(E)</b> 1000/mo-AFIL/N	1,000	AU			
70	<b>(b) (7)(E)</b> 1000/mo-AFIL/N	1,000	AU			

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		TOT. (Cont. pages)
21. MAIL INVOICE TO:				
SEE BILLING	a. NAME DHS - Customs & Border Protection	National Finance Center		<b>(b) (4)</b>
INSTRUCTIONS	b. STREET ADDRESS (or P.O. Box) PO Box 68908			17(i) GRAND TOTAL
REVERSE	c. CITY Indianapolis	d. STATE IN	e. ZIP CODE 46268	

22. UNITED STATES OF AMERICA BY <b>(b) (6)</b>	23. NAME (Typed) SUSAN E. HARGETT-EVANS TITLE: CONTRACTING/ORDERING OFFICER	(REV.)
---	---	--------

**ORDER FOR SUPPLIES OR SERVICES**  
**Schedule - Continuation**

PAGE OF PAGES  
 2 5

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

1. DATE OF ORDER 08/16/2010	2. CONTRACT NO. (if any) HSHQDC07D00021	3. ORDER NO. HSBP1010J00572
--------------------------------	--	--------------------------------

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Acpt
80	(b) (7)(E) -1000/mo-AFI L/N	1.000	AU	(b) (4)	(b) (4)	
90	(b) (7)(E) -1000/mo-AFI L/N	1.000	AU			
100	(b) (7)(E) -1000/mo-AFI L/N	1.000	AU			
110	Lexis.com Flat Rate - AFI/LN	1.000	AU			

DATE OF ORDER 08/16/2010	CONTRACT NO. (if any) HSHQDC07D00021	ORDER NO. HSBP1010J00572	PAGE 3	OF 5	PAGES
-----------------------------	---	-----------------------------	-----------	---------	-------

**Federal Tax Exempt ID: 72-0408780**

**Emailing Invoices to CBP.** As an alternative to mailing invoices to the National Finance Center as shown on page one of this award you may email invoices to: [cbpinvoices@dhs.gov](mailto:cbpinvoices@dhs.gov).

**NOTES:**

The purpose of this delivery order is to provide line items 00010 through 00110 per the terms and conditions of DHS FirstSource Contract No. HSHQDC-07-D-00021.

Reference FedBid Bid No. 8335616 for Buy No. 197919\_04 dated 8/2/10.

The period of performance is from September 29, 2010 to September 30, 2011.

The Order Number (Block 3) shall be referenced on the invoice.

Send invoice to the address in Block 21 or e-mail to [cbpinvoices@dhs.gov](mailto:cbpinvoices@dhs.gov) and to: Office of Intelligence, Attn: (b) (6), Dir. Intel Advanced Analytics Advanced Analysis, Intel Systems Office of Intelligence Operations Coordination, U.S. Customs and Border Protection, Department of Homeland Security, 5971 Kingstowne Village Pkwy, Ste 500F, Alexandria, VA 20598, Ph. (b) (6) and to: (b) (6), Budget Officer, U.S. Customs and Border Protection, Office of Intelligence and Operations Coordination Mission Support Division, 1300 Pennsylvania Avenue, NW, Ste 7.2A#9, Washington DC 20229, (b) (6), Ph. (b) (6)

CBP Delivery Site Point of Contact: (b) (6)

Contract Specialist: (b) (6)

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA  
FOR  
DELIVERY ORDER: HSBP1010J00572**

**I.1 SCHEDULE OF SUPPLIES/SERVICES**

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	(b) (7)(E) 13,000 - AFI L/N	1.000	AU	(b)	(4)
20	(b) (7)(E) 4,000 - AFI/LN	1.000	AU		
30	(b) (7)(E) 13,000 - AFI L/N	1.000	AU		
40	(b) (7)(E) -1000 hits/mo-AFI L/N	1.000	AU		
50	(b) (7)(E) -1000 hits/mo-AFI L/N	1.000	AU		
60	(b) (7)(E) -1000/mo-AFI L/N	1.000	AU		
70	(b) (7)(E) -1000/mo-AFI L/N	1.000	AU		
80	(b) (7)(E) -1000/mo-AFI L/N	1.000	AU		
90	(b) (7)(E) -1000/mo-AFI L/N	1.000	AU		
100	(b) (7)(E) -1000/mo-AFI L/N	1.000	AU		
110	Lexis.com Flat Rate (GOVLAW & WGVLAW) For 3 user IDs- AFI/LN #9001GT	1.000	AU		

**Total Funded Value of Award:**

**\$516,628.56**

**I.2 ACCOUNTING and APPROPRIATION DATA**

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	(b) (4)
20	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	
30	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	
40	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	
50	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	
60	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	
70	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	
80	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	
90	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	
100	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	
110	6100.2525USCSGLCS0925030400Z00010400HQ01 400022525	

**I.3 DELIVERY SCHEDULE**

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 5971 Kingstown Village Parkway Alexandria, VA 22315	10	1.000	09/30/2010
	20	1.000	09/30/2010
	30	1.000	09/30/2010
	40	1.000	09/30/2010

<b>DELIVER TO:</b>	<b>ITEM #</b>	<b>QTY</b>	<b>DELIVERY DATE</b>
	50	1.000	09/30/2010
	60	1.000	09/30/2010
	70	1.000	09/30/2010
	80	1.000	09/30/2010
	90	1.000	09/30/2010
	100	1.000	09/30/2010
	110	1.000	09/30/2010

# ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 3

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

1. DATE OF ORDER 12/29/12	2. CONTRACT NO. (if any) HSHQDC07D00020	6. SHIP TO: a. NAME OF CONSIGNEE See Attached Delivery Schedule	
3. ORDER NO. HSBP1012J00087	4. REQUISITION/REFERENCE NO. 0020067224	b. STREET ADDRESS	
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		c. CITY	e. ZIP CODE
7. TO:		8. TYPE OF ORDER	
a. NAME OF CONTRACTOR ALL POINTS LOGISTICS INC		<input type="checkbox"/> 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.	<input checked="" type="checkbox"/> b. DELIVERY -- Except for bifling 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.
b. COMPANY NAME		10. REQUISITIONING OFFICE <b>(b) (6)</b>	
c. STREET ADDRESS 4901 CORPORATE DR NW STE G		9. ACCOUNTING AND APPROPRIATION DATA 6100.2574USCSGLCS0923060000Z00012400HQ0104010300	
d. CITY HUNTSVILLE	e. STATE AL	f. ZIP CODE 35805-6219	

11. BUSINESS CLASSIFICATION (Check appropriate box(es))			12. F.O.B. POINT
<input checked="" type="checkbox"/> a. SMALL	<input type="checkbox"/> b. OTHER THAN SMALL	<input type="checkbox"/> c. DISADVANTAGED	Destination
<input type="checkbox"/> d. WOMEN-OWNED	<input type="checkbox"/> e. HUBZone	<input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED	
<input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN- OWNED SMALL BUSINESS PROGRAM	<input type="checkbox"/> h. ECONOMICALLY DISADVANTAGED WOMEN- OWNED SMALL BUSINESS (EDWOSB)	16. DISCOUNT TERMS Net 30	
13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 01/20/12
a. INSPECTION DESTINATION	b. ACCEPTANCE DESTINATION		

17. SCHEDULE (See reverse for Rejections)						
ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Accept
10	<b>(b) (7)(E)</b> 13,000	1,000	AU		<b>(b) (4)</b>	
20	<b>(b) (7)(E)</b> 4,000	1,000	AU			
30	<b>(b) (7)(E)</b> 13,000	1,000	AU			
40	<b>(b) (7)(E)</b> 1,000	1,000	AU			
50	<b>(b) (7)(E)</b> 1,000	1,000	AU			
60	<b>(b) (7)(E)</b> 1,000	1,000	AU			
70	<b>(b) (7)(E)</b> 1,000	1,000	AU			

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	<b>(b) (4)</b>	17(h)TOT. (Cont. pages)
21. MAIL INVOICE TO:				
a. NAME DHS - Customs & Border Protection National Finance Center			\$424,903.18	17(i) GRAND TOTAL
b. STREET ADDRESS (or P.O. Box) PO Box 68908				
c. CITY Indianapolis		d. STATE IN	e. ZIP CODE 46268	

22. UNITED STATES OF AMERICA BY (Signature) <b>(b) (6)</b>	23. NAME (Typed) HERMAN SHIVERS TITLE: CONTRACTING/ORDERING OFFICER
--	---

**ORDER FOR SUPPLIES OR SERVICES**  
**Schedule - Continuation**

PAGE OF PAGES  
 2 3

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

1. DATE OF ORDER 12/29/12	2. CONTRACT NO. (if any) HSHQDC07D00020	3. ORDER NO. HSBP1012J00087
------------------------------	--	--------------------------------

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Account
80	(b) (7)(E) 1,000	1,000	AU	(b) (4)	(b) (4)	
90	(b) (7)(E) 1,000	1,000	AU			

DATE OF ORDER 12/29/12	CONTRACT NO. (if any) HSHQDC07D00020	ORDER NO. HSBP1012J00087	PAGE OF PAGES 3 3
---------------------------	---	-----------------------------	----------------------

**Federal Tax Exempt ID: 72-0408780**

**Emailing Invoices to CBP.** As an alternative to mailing invoices to the National Finance Center as shown on page one of this award you may email invoices to: [cbpinvoices@dhs.gov](mailto:cbpinvoices@dhs.gov).

**NOTES:**

The firm fixed price delivery order, HSBP1012J00087 is issued against the Department of Homeland Security contract HSHQDC-07-D-00020 for Renewal of Database Access & Search Tools in accordance with the attached Bill of Materials.

The period of performance is 01/01/2012 through 12/31/2012. Delivery is required on or before 01/20/2012.

Reference: All Points Logistics, Inc bid#13786844 for buy#312822 on Fedbid issued by (b) (6).

The technical point of contact for this order is: (b) (6)

The contracting point of contact is: Herman T. Shivers at (b) (6)

See attached Bill of Materials for details.

Please submit all invoices to each of the following:

[Cbpinvoices@dhs.gov](mailto:Cbpinvoices@dhs.gov)

(b) (6)

DHS – Customs and Border Protection  
National Finance Center  
(Address in Section 21 of this delivery order)



**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA  
FOR  
DELIVERY ORDER: HSBP1012J00087**

**I.1 SCHEDULE OF SUPPLIES/SERVICES**

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	(b) (7) (E) 13,000	1.000	AU	(b) (4)	(4)
20	(b) (7) (E) 4,000	1.000	AU		
30	(b) (7) (E) 13,000	1.000	AU		
40	(b) (7) (E) 1,000	1.000	AU		
50	(b) (7) (E) 1,000	1.000	AU		
60	(b) (7) (E) 1,000	1.000	AU		
70	(b) (7) (E) 1,000	1.000	AU		
80	(b) (7) (E) 1,000	1.000	AU		
90	(b) (7) (E) 1,000	1.000	AU		

**Total Funded Value of Award:**

**\$424,903.18**

**I.2 ACCOUNTING and APPROPRIATION DATA**

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2574USCSGLCS0923060000Z00012400HQ0104010300 IU5012574	(b) (4)
20	6100.2574USCSGLCS0923060000Z00012400HQ0104010300 IU5012574	
30	6100.2574USCSGLCS0923060000Z00012400HQ0104010300 IU5012574	
40	6100.2574USCSGLCS0923060000Z00012400HQ0104010300 IU5012574	
50	6100.2574USCSGLCS0923060000Z00012400HQ0104010300 IU5012574	
60	6100.2574USCSGLCS0923060000Z00012400HQ0104010300 IU5012574	
70	6100.2574USCSGLCS0923060000Z00012400HQ0104010300 IU5012574	
80	6100.2574USCSGLCS0923060000Z00012400HQ0104010300 IU5012574	
90	6100.2574USCSGLCS0923060000Z00012400HQ0104010300 IU5012574	

**I.3 DELIVERY SCHEDULE**

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 5971 Kingstown Village Parkway Alexandria, VA 22315	10	1.000	12/30/2011
	20	1.000	12/30/2011
	30	1.000	12/30/2011
	40	1.000	12/30/2011
	50	1.000	12/30/2011
	60	1.000	12/30/2011
	70	1.000	12/30/2011
	80	1.000	12/30/2011
	90	1.000	12/30/2011

**I.4 LIMITATION OF GOVERNMENT'S OBLIGATION DURING A CONTINUING RESOLUTION (SEP 2011) (HSAM DEVIATION)**

The following information must be included in a contract or order when incremental funding of fixed price, Time and Materials and Labor Hours contracts is authorized when the component is operating under a CR. Contract line item(s) listed below are incrementally funded or fully funded as shown in the below table. For these item(s), the sum of \$ [Insert after Negotiation] of the total price is presently available for payment and allotted to this contract. This funding will be updated in each contract modification.

**INSERT TABLE HERE**

- (b) For item(s) identified in paragraph (a) as not fully funded, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement of authorized termination costs in the event of termination of those item(s) for the Government's convenience, does not exceed the total amount currently allotted to the items not fully funded under the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The total amount payable by the Government in the event of such termination of those contract line item(s) identified in paragraph (a) above includes costs, profit, and estimated/negotiated termination settlement costs for those item(s). The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the line items of the contract regardless of anything to the contrary in any other clause, such as the clause entitled "Termination for Convenience of the Government" or paragraph (l) entitled "Termination for the Government's Convenience" of the clause at FAR 52.212-4, "Commercial Terms and Conditions-Commercial Items."
- (c) Notwithstanding paragraph (i) of this requirement, the Contractor will notify the Contracting Officer in writing at least thirty days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this contract. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract authorizing termination for the convenience of the government, such as the clause entitled "Termination for Convenience of the Government" or paragraph (l) entitled "Termination for the Government's Convenience" of the clause at FAR 52.212-4, "Commercial Terms and Conditions-Commercial Items."
- (d) When additional funds are allotted for continued performance of the contract line item(s) identified in paragraph (a), the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of paragraphs (b) through (d) will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.
- (e) The Government may at any time prior to termination allot additional funds for the performance of the contract line item(s) identified in paragraph (a).
- (f) The termination provisions of paragraphs (a) through (i) do not limit the rights of the Government under the clause entitled "Default" or "Termination for Cause." The provisions of this clause are limited to the work and allotment of funds for the contract line item(s) set forth in paragraph (a). This clause no longer applies once the contract is fully funded.
- (g) Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government" or paragraph (l) entitled "Termination for the Government's Convenience" of the clause at FAR 52.212-4, "Commercial Terms and Conditions-Commercial Items."
- (h) Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.
- (i) The parties contemplate that the Government will allot funds to this contract from time to time as the need arises and as funds become available. There is no fixed schedule for providing additional funds.

(End of Clause)

## **1.5 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)**

- 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]

**I.6 52.227-19 COMMERCIAL COMPUTER SOFTWARE LICENSE (DEC 2007)**

# ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 3

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

1. DATE OF ORDER 12/19/2012	2. CONTRACT NO. (if any) HSHQDC-12-D-00022	6. SHIP TO:	
3. ORDER NO. HSBP1013J00065	4. REQUISITION/REFERENCE NO. 0020072259	a. NAME OF CONSIGNEE See Attached Delivery Schedule	
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		b. STREET ADDRESS	
		c. CITY	d. STATE e. ZIP CODE
		f. SHIP VIA	

7. TO:		8. TYPE OF ORDER	
a. NAME OF CONTRACTOR AKIRA TECHNOLOGIES INC		<input type="checkbox"/> 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.	<input checked="" type="checkbox"/> 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.
b. COMPANY NAME <b>(b) (6)</b>			
c. STREET ADDRESS 10 G ST NE STE 710			
d. CITY WASHINGTON	e. STATE DC	f. ZIP CODE 20002-4288	

9. ACCOUNTING AND APPROPRIATION DATA		10. REQUISITIONING OFFICE TASPO	
--------------------------------------	--	------------------------------------	--

11. BUSINESS CLASSIFICATION (Check appropriate box(es))			12. F.O.B. POINT
<input checked="" type="checkbox"/> a. SMALL	<input type="checkbox"/> b. OTHER THAN SMALL	<input checked="" type="checkbox"/> c. DISADVANTAGED	Not applicable
<input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED	<input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM	<input type="checkbox"/> d. WOMEN-OWNED	
			<input type="checkbox"/> e. HUBZone
			<input type="checkbox"/> h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 01/01/2013	16. DISCOUNT TERMS Net 30
a. INSPECTION DESTINATION	b. ACCEPTANCE DESTINATION			

17. SCHEDULE (See reverse for Rejections)						
ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Acpt
10	<b>(b) (7)(E)</b> 13,000	1.000	AU		<b>(b) (4)</b>	
20	<b>(b) (7)(E)</b> 4,000	1.000	AU			
30	<b>(b) (7)(E)</b> 13,000	1.000	AU			
40	<b>(b) (7)(E)</b> 1,000	1.000	AU			
50	<b>(b) (7)(E)</b> 1,000	1.000	AU			
60	<b>(b) (7)(E)</b> 1,000	1.000	AU			
70	<b>(b) (7)(E)</b> 1,000	1.000	AU			

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		<b>(b) (4)</b>	17(h)TOT. (Cont. pages)
21. MAIL INVOICE TO:							\$411,388.35
SEE BILLING INSTRUCTIONS REVERSE		a. NAME DHS - Customs & Border Protection National Finance Center					
		b. STREET ADDRESS (or P.O. Box) <b>(b) (6)</b> x 68908					
		c. CITY Indianapolis	d. STATE IN	e. ZIP CODE 46268			

22. UNITED STATES OF AMERICA BY (Signature)		23. NAME (Typed) ROBERT ABOOD TITLE: CONTRACTING/ORDERING OFFICER	
---	--	---	--

**ORDER FOR SUPPLIES OR SERVICES  
Schedule - Continuation**

PAGE OF PAGES

2 3

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

1. DATE OF ORDER  
12/19/2012

2. CONTRACT NO. (if any)  
HSHQDC-12-D-00022

3. ORDER NO.  
HSBP1013J00065

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Acpt
80	(b) (7)(E) 000	1.000	AU		(b) (4)	
90	000	1.000	AU		(b) (4)	

DATE OF ORDER 12/19/2012	CONTRACT NO. (if any) HSHQDC-12-D-00022	ORDER NO. HSBP1013J00065	PAGE OF PAGES 3 3
-----------------------------	--	-----------------------------	----------------------

**Federal Tax Exempt ID: 72-0408780**

**Emailing Invoices to CBP.** As an alternative to mailing invoices to the National Finance Center as shown on page one of this award you may email invoices to: [cbpinvoices@dhs.gov](mailto:cbpinvoices@dhs.gov).

**NOTES:**

The firm fixed price delivery order, HSBP1013J00065 is issued against the Department of Homeland Security contract HSHQDC-12-D-00022 for the Renewal of Database Access and Search Tools as described in the Statement of Work.

The period of performance is 01/01/2013 through 12/31/2013. Delivery is required on or before 01/01/2013.

Reference Akira Technologies Inc. Bid# 19369050 / Buy# 438842\_01 on FedBid issued by (b) (6)

The Technical Point of Contact for this order is: (b) (6)

The Contracting Point of contact is: (b) (6)

See attached Statement of Work for details.

Please submit all invoices to each of the following:

[cbpinvoices@dhs.gov](mailto:cbpinvoices@dhs.gov)

(b) (6)

DHS - Customs and Border Protection  
National Finance Center  
(Address in Section 21 of this Delivery Order)

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA  
FOR  
DELIVERY ORDER: HSBP1013J00065**

**I.1 SCHEDULE OF SUPPLIES/SERVICES**

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	(b) (7)(E) 13,000	1.000	AU	<b>(b) (4)</b>	<b>(4)</b>
20	(b) (7)(E) 4,000	1.000	AU		
30	(b) (7)(E) 13,000	1.000	AU		
40	(b) (7)(E) 1,000	1.000	AU		
50	(b) (7)(E) 1,000	1.000	AU		
60	(b) (7)(E) 1,000	1.000	AU		
70	(b) (7)(E) 1,000	1.000	AU		
80	(b) (7)(E) 1,000	1.000	AU		
90	(b) (7)(E) 1,000	1.000	AU		

**Total Funded Value of Award:**

**\$411,388.35**

**I.2 ACCOUNTING and APPROPRIATION DATA**

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2574USCSGLCS0923060000Z00013400HQ011402AC00 IU5442574	<b>(b) (4)</b>
20	6100.2574USCSGLCS0923060000Z00013400HQ011402AC00 IU5442574	
30	6100.2574USCSGLCS0923060000Z00013400HQ011402AC00 IU5442574	
40	6100.2574USCSGLCS0923060000Z00013400HQ011402AC00 IU5442574	
50	6100.2574USCSGLCS0923060000Z00013400HQ011402AC00 IU5442574	
60	6100.2574USCSGLCS0923060000Z00013400HQ011402AC00 IU5442574	
70	6100.2574USCSGLCS0923060000Z00013400HQ011402AC00 IU5442574	
80	6100.2574USCSGLCS0923060000Z00013400HQ011402AC00 IU5442574	
90	6100.2574USCSGLCS0923060000Z00013400HQ011402AC00 IU5442574	

**I.3 DELIVERY SCHEDULE**

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 5971 Kingstown Village Parkway Alexandria, VA 22315	10	1.000	01/01/2013
	20	1.000	01/01/2013
	30	1.000	01/01/2013
	40	1.000	01/01/2013
	50	1.000	01/01/2013
	60	1.000	01/01/2013
	70	1.000	01/01/2013
	80	1.000	01/01/2013
	90	1.000	01/01/2013

**I.4 3052.209-70 PROHIBITION ON CONTRACTS WITH CORPORATE EXPATRIATES (JUN 2006)**

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

## (b) Definitions. As used in this clause:

*Expanded Affiliated Group* means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting 'more than 50 percent' for 'at least 80 percent' each place it appears.

*Foreign Incorporated Entity* means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

*Inverted Domestic Corporation.* A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

- (1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;
- (2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—
  - (i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or
  - (ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and
- (3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

*Person, domestic, and foreign* have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

## (c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

- (1) *Certain stock disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:
  - (i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or
  - (ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).
- (2) *Plan deemed in certain cases.* If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.
- (3) *Certain transfers disregarded.* The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special rule for related partnerships.* For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395 (b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

## (e) Treatment of Certain Rights.



(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

- (i) warrants;
- (ii) options;
- (iii) contracts to acquire stock;
- (iv) convertible debt instruments; and
- (v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of section 835.

(f) *Disclosure.* The offeror under this solicitation represents that [Check one]:

it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of Clause)

**I.5 52.232-99 PROVIDING ACCELERATED PAYMENT TO SMALL BUSINESS SUBCONTRACTORS (DEVIATION)**

This clause implements the temporary policy provided by OMB Policy Memorandum *M-12-16, Providing Prompt Payment to Small Business Subcontractors*, dated July 11, 2012.

- (a) Upon receipt of accelerated payments from the Government, the contractor is required to make accelerated payments to small business subcontractors to the maximum extent practicable after receipt of a proper invoice and all proper documentation from the small business subcontractor.
- (b) Include the substance of this clause, including this paragraph (b), in all subcontracts with small business concerns.
- (c) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(End of clause)

**I.6 PAYMENT AND INVOICE INSTRUCTIONS (FEB 2012)**

In order to request contract payment, the contractor shall submit a proper invoice, as defined by Federal Acquisition Regulation (FAR) 2.101 for payment in the manner and format described below.

**SUBMISSION OF INVOICES**

(a) The contractor shall submit an original invoice/voucher, via postal mail or electronic mail (email), simultaneously to the following:

(1) National Finance Center (NFC)

DHS/U.S. Customs and Border Protection  
National Finance Center/Commercial Accounts  
PO Box 68908  
Indianapolis, Indiana 46268

OR email: cbpinvoices@dhs.gov

**NOTE: For invoices with payment terms less than net 30, the subject line for all emailed invoices to the NFC must include the following text: "Per CBP, Net [state # days] Invoice".**

- (2) Contracting Officer or Contract Administrator (CO or CA) *[fill in at time of award]*

DHS/U.S. Customs and Border Protection  
Attention: Robert F. Abood

OR email: (b) (6)

- (3) Contracting Officer's Representative (COR) *[fill in at time of award]*

DHS/U.S. Customs and Border Protection  
Attention: (b) (6)

OR email: (b) (6)

- (b) The contractor shall submit a copy of the original invoice/voucher for all DHS cost-reimbursement and time and material/labor hour contracts and delivery orders to the branch manager/resident auditor of the cognizant Defense Contract Audit Agency (DCAA) Field Audit Office. Copies may be sent to DCAA, via postal mail or email and must be sent at the same time the invoice/voucher is sent to the NFC, CO and COR. The CO shall provide the following information:

DCAA Field Office  
Attention:

Phone:

Email:

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

#### INVOICE REVIEW AND APPROVAL REQUIREMENTS

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

- (1) The minimum requirements are:

- i. Name and address of the contractor.
- ii. Invoice date and invoice number.
- iii. Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).
- iv. Description, quantity, unit of measure, unit price, and extended price of supplies delivered or services performed.
- v. Shipping and payment terms (e.g. shipment number and date of shipment, discount for prompt payment terms). Bill of lading number and weight of shipment will be shown for shipments on Government bills of lading.

- vi. Name and address of contractor official to whom payment is to be sent (must be the same as that in the contract or in a proper notice of assignment).
  - vii. Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
  - viii. Taxpayer identification number (TIN).
  - ix. Electronic funds transfer (EFT) banking information.
  - x. Any other information or documentation required by the contract (e.g. evidence of shipment).
- (2) For cost reimbursement or time and material contracts (other than a contract for a commercial item), the contractor shall bill and maintain a record of indirect costs in accordance with FAR 52.216-7(d).
- (b) Supplemental documentation required for review and approval of invoices, at the written direction of the contracting officer, may be submitted directly to either the contracting officer, or the contracting officer's representative. Contractors shall submit all supplemental invoice documentation along with the original invoice.
- (c) Invoices that fail to provide the information required by the Prompt Payment clause (FAR 52.232-25) may be rejected by the Government and returned to the contractor.

**ADDITIONAL INVOICE REQUIREMENTS**

In addition to the invoice requirements contained in FAR 32.905 and FAR 52.216-7, the following also applies:

- (1) Invoices must include the following information to support all costs claimed:
  - i. Period of performance for the costs claimed;
  - ii. Current amounts for each CLIN, if applicable;
  - iii. Current direct and indirect incurred costs, including fee;
  - iv. Cumulative amounts for each CLIN; and
  - v. Statement signed by an authorized company representative certifying that the costs in the invoice are accurate and complete.
- (2) The Government reserves the right to make invoice adjustments if associated costs are determined to be unallowable.

[End of Clause]

**I.7 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]

# ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 3

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

1. DATE OF ORDER 12/27/2013	2. CONTRACT NO. (if any) HSHQDC-13-D-00012	6. SHIP TO:		
3. ORDER NO. HSBP1014J00039		4. REQUISITION/REFERENCE NO. 0020077614		
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		a. NAME OF CONSIGNEE See Attached Delivery Schedule		
		b. STREET ADDRESS		
		c. CITY	d. STATE	e. ZIP CODE
7. TO:		f. SHIP VIA		
a. NAME OF CONTRACTOR PAN AMERICA COMPUTERS INC		8. TYPE OF ORDER		
b. COMPANY NAME		<input type="checkbox"/> 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.		
c. STREET ADDRESS 205 EAST MAIN ST STE 2		<input checked="" type="checkbox"/> 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.		
d. CITY FRONT ROYAL	e. STATE VA	f. ZIP CODE 22630		
9. ACCOUNTING AND APPROPRIATION DATA SEE ATTACHED		10. REQUISITIONING OFFICE <b>(b) (6)</b>		

11. BUSINESS CLASSIFICATION (Check appropriate box(es))			12. F.O.B. POINT	
<input checked="" type="checkbox"/> a. SMALL	<input type="checkbox"/> b. OTHER THAN SMALL	<input type="checkbox"/> c. DISADVANTAGED	<input checked="" type="checkbox"/> d. WOMEN-OWNED	<input type="checkbox"/> e. HUBZone
<input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED	<input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM		<input type="checkbox"/> h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)	
13. PLACE OF			14. GOVERNMENT B/L NO.	
a. INSPECTION		b. ACCEPTANCE		
15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 01/01/2014			16. DISCOUNT TERMS Net 30	

**17. SCHEDULE (See reverse for Rejections)**

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Acct
10	<b>(b) (7)(E)</b> 13,000	1.000	AU	<b>(b) (4)</b>		
20	<b>(b) (7)(E)</b> 4,000	1.000	AU			
30	<b>(b) (7)(E)</b> 13,000	1.000	AU			
40	<b>(b) (7)(E)</b> 1,000	1.000	AU			
50	<b>(b) (7)(E)</b> 1,000	1.000	AU			
60	<b>(b) (7)(E)</b> 1,000	1.000	AU			
70	<b>(b) (7)(E)</b> 1,000	1.000	AU			

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		<b>(b) (4)</b>	17(h)TOT. (Cont. pages)
21. MAIL INVOICE TO:					
a. NAME DHS - Customs & Border Protection		National Finance Center		\$407,647.30	17(i) GRAND TOTAL
b. STREET ADDRESS (or P.O. Box) PO Box 68908					
c. CITY Indianapolis	d. STATE IN	e. ZIP CODE 46268			

22. UNITED STATES OF AMERICA BY (Signature) <b>(b) (6)</b>	23. NAME (Typed) Hyun Jung Koo TITLE: CONTRACTING/ORDERING OFFICER
--	--

**ORDER FOR SUPPLIES OR SERVICES  
Schedule - Continuation**

PAGE OF PAGES

2 3

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

1. DATE OF ORDER  
12/27/2013

2. CONTRACT NO. (if any)  
HSHQDC-13-D-00012

3. ORDER NO.  
HSBP1014J00039

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Accpt
80	(b) (7)(E) 1,000	1.000	AU	(b) (4)	(b) (4)	
90	1,000	1.000	AU	(b) (4)	(b) (4)	

DATE OF ORDER 12/27/2013	CONTRACT NO. (if any) HSHQDC-13-D-00012	ORDER NO. HSBP1014J00039	PAGE OF PAGES 3 3
-----------------------------	--	-----------------------------	----------------------

**Federal Tax Exempt ID: 72-0408780**

**Emailing Invoices to CBP.** As an alternative to mailing invoices to the National Finance Center as shown on page one of this award you may email invoices to: [cbpinvoices@dhs.gov](mailto:cbpinvoices@dhs.gov).

**NOTES:**

This firm fixed price order (HSBP1014J00039) for the renewal of LexisNexis database access and search tools as described in the Statement of Work. This delivery order is issued by the U.S. Customs and Border Protection (CBP), against the Department of Homeland Security(DHS) FirstSource II IDIQ, HSHQDC-13-D-00012, to Panamerica Computers, Inc. (DUNS (b) (4) CAGE Code: (b) (4).

All terms and conditions of both the Customs and Border Protection (CBP) delivery order and the DHS FirstSource II IDIQ are in full effect.

The requirement, as represented in line items #00010-00090, is hereby fully funded for a total order value of \$407,647.30. Incorporated by reference is Panamerica Computers Inc. Bid# 25371196 / Buy# 579494\_03 on FedBid issued by (b) (6)

The period of performance is 01/01/2014 through 12/31/2014. Delivery is required on or before 01/01/2014.

**DELIVERY ADDRESS:**

Multiple locations - see Statement of Work

**POINTS OF CONTACT:**

TASPD: (b) (6)  
COR: (b) (6)

Please send invoices to:  
National Finance Center (NFC) at [CBPinvoices@cbp.dhs.gov](mailto:CBPinvoices@cbp.dhs.gov) (Address in Section 21 of this delivery order)  
[CBPINVOICES@cbp.dhs.gov](mailto:CBPINVOICES@cbp.dhs.gov)  
Budget POC (b) (6)  
Contract Specialist: (b) (6)

All contracting questions may be directed to the Contract Specialist: (b) (6)

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA  
FOR  
DELIVERY ORDER: HSBP1014J00039**

**I.1 SCHEDULE OF SUPPLIES/SERVICES**

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	(b) (7)(E) 13,000	1.000	AU	(b) (4)	(4)
20	(b) (7)(E) 4,000	1.000	AU		
30	(b) (7)(E) 13,000	1.000	AU		
40	(b) (7)(E) 1,000	1.000	AU		
50	(b) (7)(E) 1,000	1.000	AU		
60	(b) (7)(E) 1,000	1.000	AU		
70	(b) (7)(E) 1,000	1.000	AU		
80	(b) (7)(E) 1,000	1.000	AU		
90	(b) (7)(E) 1,000	1.000	AU		

**Total Funded Value of Award:**

**\$407,647.30**

**I.2 ACCOUNTING and APPROPRIATION DATA**

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2574USCSGLCS0923060000Z00014400HQ071402AC00 IU5442574	(b) (4)
20	6100.2574USCSGLCS0923060000Z00014400HQ071402AC00 IU5442574	
30	6100.2574USCSGLCS0923060000Z00014400HQ071402AC00 IU5442574	
40	6100.2574USCSGLCS0923060000Z00014400HQ071402AC00 IU5442574	
50	6100.2574USCSGLCS0923060000Z00014400HQ071402AC00 IU5442574	
60	6100.2574USCSGLCS0923060000Z00014400HQ071402AC00 IU5442574	
70	6100.2574USCSGLCS0923060000Z00014400HQ071402AC00 IU5442574	
80	6100.2574USCSGLCS0923060000Z00014400HQ071402AC00 IU5442574	
90	6100.2574USCSGLCS0923060000Z00014400HQ071402AC00 IU5442574	

**I.3 DELIVERY SCHEDULE**

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 5971 Kingstown Village Parkway Alexandria, VA 22315	10	1.000	01/01/2014
	20	1.000	01/01/2014
	30	1.000	01/01/2014
	40	1.000	01/01/2014
	50	1.000	01/01/2014
	60	1.000	01/01/2014
	70	1.000	01/01/2014
	80	1.000	01/01/2014
	90	1.000	01/01/2014

**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 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.7 3052.209-70 PROHIBITION ON CONTRACTS WITH CORPORATE EXPATRIATES (JUN 2006)**

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

*Expanded Affiliated Group* means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting 'more than 50 percent' for 'at least 80 percent' each place it appears.

*Foreign Incorporated Entity* means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

*Inverted Domestic Corporation.* A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

- (1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;
- (2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—
  - (i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or
  - (ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and
- (3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

*Person, domestic, and foreign* have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) *Special rules.* The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

- (1) *Certain stock disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:
  - (i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or
  - (ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).
- (2) *Plan deemed in certain cases.* If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.
- (3) *Certain transfers disregarded.* The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special rule for related partnerships.* For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395 (b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) *Treatment of Certain Rights.*

- (1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:
  - (i) warrants;
  - (ii) options;
  - (iii) contracts to acquire stock;
  - (iv) convertible debt instruments; and
  - (v) others similar interests.
- (2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of section 835.

(f) *Disclosure*. The offeror under this solicitation represents that [Check one]:

it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of Clause)

#### **I.8 52.232-99 PROVIDING ACCELERATED PAYMENT TO SMALL BUSINESS SUBCONTRACTORS (DEVIATION)**

This clause implements the temporary policy provided by OMB Policy Memorandum *M-12-16, Providing Prompt Payment to Small Business Subcontractors*, dated July 11, 2012.

(a) Upon receipt of accelerated payments from the Government, the contractor is required to make accelerated payments to small business subcontractors to the maximum extent practicable after receipt of a proper invoice and all proper documentation from the small business subcontractor.

(b) Include the substance of this clause, including this paragraph (b), in all subcontracts with small business concerns.

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

(End of clause)

#### **I.9 TERM OF CONTRACT (MARCH 2003)**

The term of this contract is from 01/01/2014 through 12/31/2014.

[End of Clause]

#### **I.10 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.11 PAYMENT AND INVOICE INSTRUCTIONS (FEB 2012)**

In order to request contract payment, the contractor shall submit a proper invoice, as defined by Federal Acquisition Regulation (FAR) 2.101 for payment in the manner and format described below.

#### **SUBMISSION OF INVOICES**

(a) The contractor shall submit an original invoice/voucher, via postal mail or electronic mail (email), simultaneously to the following:

(1) National Finance Center (NFC)

DHS/U.S. Customs and Border Protection  
National Finance Center/Commercial Accounts  
PO Box 68908  
Indianapolis, Indiana 46268

OR email: cbpinvoices@dhs.gov

**NOTE: For invoices with payment terms less than net 30, the subject line for all emailed invoices to the NFC must include the following text: "Per CBP, Net [state # days] Invoice".**

(2) Contracting Officer or Contract Administrator (CO or CA) HYUN KOO

email: (b) (6)

(3) Contracting Officer's Representative (COR) (b) (6)

email: (b) (6)

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

#### INVOICE REVIEW AND APPROVAL REQUIREMENTS

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

(1) The minimum requirements are:

- i. Name and address of the contractor.
- ii. Invoice date and invoice number.
- iii. Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).
- iv. Description, quantity, unit of measure, unit price, and extended price of supplies delivered or services performed.
- v. Shipping and payment terms (e.g. shipment number and date of shipment, discount for prompt payment terms). Bill of lading number and weight of shipment will be shown for shipments on Government bills of lading.
- vi. Name and address of contractor official to whom payment is to be sent (must be the same as that in the contract or in a proper notice of assignment).
- vii. Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
- viii. Taxpayer identification number (TIN).
- ix. Electronic funds transfer (EFT) banking information.
- x. Any other information or documentation required by the contract (e.g. evidence of shipment).

(2) For cost reimbursement or time and material contracts (other than a contract for a commercial item), the contractor shall bill and maintain a record of indirect costs in accordance with FAR 52.216-7(d).

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

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

#### ADDITIONAL INVOICE REQUIREMENTS

In addition to the invoice requirements contained in FAR 32.905 and FAR 52.216-7, the following also applies:

- (1) Invoices must include the following information to support all costs claimed:
  - i. Period of performance for the costs claimed;
  - ii. Current amounts for each CLIN, if applicable;
  - iii. Current direct and indirect incurred costs, including fee;
  - iv. Cumulative amounts for each CLIN; and
  - v. Statement signed by an authorized company representative certifying that the costs in the invoice are accurate and complete.
- (2) The Government reserves the right to make invoice adjustments if associated costs are determined to be unallowable.

[End of Clause]

### **I.12 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.13 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.

[End of Clause]

#### **I.14 POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE (JUL 2010)**

##### **a. Contractor Performance Evaluation**

Interim and final performance evaluation reports will be prepared on this contract or order in accordance with FAR Subpart 42.15. A final performance evaluation report will be prepared at the time the work under this contract or order is completed. In addition to the final performance evaluation report, an interim performance evaluation report will be prepared annually to coincide with the anniversary date of the contract or order.

Interim and final performance evaluation reports will be provided to the contractor via the Contractor Performance Assessment Reporting System (CPARS) after completion of the evaluation. The CPARS Assessing Official Representatives (AORs) will provide input for interim and final contractor performance evaluations. The AORs may be Contracting Officer's Technical Representatives (COTRs), project managers, and/or contract specialists. The CPARS Assessing Officials (AOs) are the contracting officers (CO) who will sign the evaluation report and forward it to the contractor representative via CPARS for comments.

The contractor representative is responsible for reviewing and commenting on proposed ratings and remarks for all evaluations forwarded by the AO. After review, the contractor representative will return the evaluation to the AO via CPARS.

The contractor representative will be given a minimum of thirty (30) days to submit written comments or a rebuttal statement. Within seven (7) days of the comment period, the contractor representative may request a meeting with the AO to discuss the evaluation report. The AO may complete the evaluation without the contractor representative's comments if none are provided within the thirty (30) day comment period. Any disagreement between the AO/CO and the contractor representative regarding the performance evaluation report will be referred to the CPARS Reviewing Officials (ROs). Once the RO completes the review, the evaluation is considered complete and the decision is final. Copies of the evaluations, contractor responses, and review comments, if any, will be retained as part of the contract file and may be used in future award decisions.

##### **b. Primary and Alternate Corporate Senior Contractor Representatives**

The contractor must identify a primary and alternate Corporate Senior Contractor Representative for this contract and provide the full name, title, phone number, email address, and business address to the CO within 30 days after award.

##### **c. Electronic access to contractor Performance Evaluations**

The AO/CO will request CPARS user access for the contractor by forwarding the contractor's primary and alternate representatives' information to the CPARS Focal Point (FP).

The FP is responsible for CPARS access authorizations for Government and contractor personnel. The FP will set up the user accounts and will create system access to CPARS.

The CPARS application will send an automatic notification to users when CPARS access is granted. In addition, contractor representatives will receive an automated email from CPARS when an evaluation report has been completed.

[End of Clause]

# ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 13

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

1. DATE OF ORDER 1/1/2015	2. CONTRACT NO. (if any) GS-02F-0048M	6. SHIP TO:	
3. ORDER NO. HSBP1015F00023		4. REQUISITION/REFERENCE NO. 0020081446	
5. ISSUING OFFICE (Address correspondence to) DHS - Customs & Border Protection Department of Homeland Security 1331 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229		a. NAME OF CONSIGNEE See Attached Delivery Schedule	
7. TO:		8. TYPE OF ORDER	
a. NAME OF CONTRACTOR REED ELSEVIER INC		<input type="checkbox"/> 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. COMPANY NAME		<input checked="" type="checkbox"/> 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.	
c. STREET ADDRESS 1150 18TH ST NW STE 600 D/B/A LEXISNEXIS		10. REQUISITIONING OFFICE  (b) (6)	
d. CITY WASHINGTON	e. STATE DC	f. ZIP CODE 20036-3843	
9. ACCOUNTING AND APPROPRIATION DATA			

11. BUSINESS CLASSIFICATION (Check appropriate box(es))					12. F.O.B. POINT
<input type="checkbox"/> a. SMALL	<input checked="" type="checkbox"/> b. OTHER THAN SMALL	<input type="checkbox"/> c. DISADVANTAGED	<input type="checkbox"/> d. WOMEN-OWNED	<input type="checkbox"/> e. HUBZone	Destination
<input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED	<input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM	<input type="checkbox"/> h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)			

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 01/01/2015	16. DISCOUNT TERMS Net 30
a. INSPECTION DESTINATION	b. ACCEPTANCE DESTINATION			

17. SCHEDULE (See reverse for Rejections)						
ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Acctp
10	(b) (7)(E) 13,000	1.000	AU	<b>(b) (4)</b>		
20	(b) (7)(E) 4,000	1.000	AU			
30	(b) (7)(E) 13,000	1.000	AU			
40	(b) (7)(E) 1,000	1.000	AU			
50	(b) (7)(E) 1,000	1.000	AU			
60	(b) (7)(E) 1,000	1.000	AU			
70	(b) (7)(E) 1,000	1.000	AU			

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		17(h)TOT. (Cont. pages)
21. MAIL INVOICE TO:						
SEE BILLING INSTRUCTIONS REVERSE	a. NAME DHS - Customs & Accounts Sect.		<b>(b) (4)</b>		\$413,280.00	
	b. STREET ADDRESS (b) (6)					
	c. CITY Indianapolis	e. ZIP CODE 46278				
22. UNITED STATES OF AMERICA BY (Signature)				23. NAME (Typed) Robert Abood TITLE: CONTRACTING/ORDERING OFFICER		17(i) GRAND TOTAL

**ORDER FOR SUPPLIES OR SERVICES  
Schedule - Continuation**

PAGE OF PAGES  
2 13

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

1. DATE OF ORDER 1/1/2015	2. CONTRACT NO. (if any) GS-02F-0048M	3. ORDER NO. HSBP1015F00023
------------------------------	--	--------------------------------

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Acpt
80	(b) (7)(E) 1,000	1.000	AU	(b) (4)	(b) (4)	
90	(b) (7)(E) 1,000	1.000	AU			



DATE OF ORDER 1/1/2015	CONTRACT NO. (if any) GS-02F-0048M	ORDER NO. HSBP1015F00023	PAGE OF PAGES 3 13
---------------------------	---------------------------------------	-----------------------------	-----------------------

**Federal Tax Exempt ID: 72-0408780**

**Emailing Invoices to CBP.** As an alternative to mailing invoices to the National Finance Center as shown on page one of this award you may email invoices to: [cbpinvoices@dhs.gov](mailto:cbpinvoices@dhs.gov).

**NOTES:**

This firm-fixed price delivery order (HSBP1015F00023) is issued against the General Services Administration's (GSA's) Schedule 76 contract, GS-02F-0048M for access to the LexisNexis database in support of Customs and Border Protection's (CBP's) Analytical Framework for Intelligence (AFI) project. The delivery order will be executed in accordance with both the proposal submitted via e-mail by LexisNexis on December 22, 2014 and the attached Statement of Work (SOW).

The Period of Performance for this order is from January 1, 2015 through December 31, 2015.

The Contracting Officer's Representative for this order is (b) (6)

The contracting point of contact is (b) (6).

Please submit all invoices to each of the following:

\*cbpinvoices@dhs.gov; or

DHS – Customs and Border Protection  
National Finance Center  
(address in Section 21 of this delivery order); and

(b) (6)

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA  
FOR  
DELIVERY ORDER: HSBP1015F00023**

**I.1 SCHEDULE OF SUPPLIES/SERVICES**

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	(b) (7)(E) 13,000	13,000	AU	(b)	(4)
20	(b) (7)(E) 4,000	4,000	AU		
30	(b) (7)(E) 13,000	13,000	AU		
40	(b) (7)(E) 1,000	1,000	AU		
50	(b) (7)(E) 1,000	1,000	AU		
60	(b) (7)(E) 1,000	1,000	AU		
70	(b) (7)(E) 1,000	1,000	AU		
80	(b) (7)(E) 1,000	1,000	AU		
90	(b) (7)(E) 1,000	1,000	AU		

Total Funded Value of Award:

\$413,280.00

**I.2 ACCOUNTING and APPROPRIATION DATA**

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2574USCSGLCS0923060000Z00015400HQ071402AE00 IU5442574 TAS# 07020152015 0530000	(b) (4)
20	6100.2574USCSGLCS0923060000Z00015400HQ071402AE00 IU5442574 TAS# 07020152015 0530000	
30	6100.2574USCSGLCS0923060000Z00015400HQ071402AE00 IU5442574 TAS# 07020152015 0530000	
40	6100.2574USCSGLCS0923060000Z00015400HQ071402AE00 IU5442574 TAS# 07020152015 0530000	
50	6100.2574USCSGLCS0923060000Z00015400HQ071402AE00 IU5442574 TAS# 07020152015 0530000	
60	6100.2574USCSGLCS0923060000Z00015400HQ071402AE00 IU5442574 TAS# 07020152015 0530000	
70	6100.2574USCSGLCS0923060000Z00015400HQ071402AE00 IU5442574 TAS# 07020152015 0530000	
80	6100.2574USCSGLCS0923060000Z00015400HQ071402AE00 IU5442574 TAS# 07020152015 0530000	
90	6100.2574USCSGLCS0923060000Z00015400HQ071402AE00 IU5442574 TAS# 07020152015 0530000	

**I.3 DELIVERY SCHEDULE**

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 5971 Kingstown Village Parkway Alexandria, VA 22315	10	1.000	01/01/2015
	20	1.000	01/01/2015
	30	1.000	01/01/2015
	40	1.000	01/01/2015
	50	1.000	01/01/2015
	60	1.000	01/01/2015
	70	1.000	01/01/2015
	80	1.000	01/01/2015
	90	1.000	01/01/2015

**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 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.7 3052.209-70 PROHIBITION ON CONTRACTS WITH CORPORATE EXPATRIATES (JUN 2006)**

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

*Expanded Affiliated Group* means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting 'more than 50 percent' for 'at least 80 percent' each place it appears.

*Foreign Incorporated Entity* means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

*Inverted Domestic Corporation.* A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

- (1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;
- (2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—
  - (i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or
  - (ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and
- (3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

*Person, domestic, and foreign* have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

- (c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.
- (1) *Certain stock disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:
    - (i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or
    - (ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).
  - (2) *Plan deemed in certain cases.* If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.
  - (3) *Certain transfers disregarded.* The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.
- (d) *Special rule for related partnerships.* For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395 (b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

- (1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

- (i) warrants;
- (ii) options;
- (iii) contracts to acquire stock;
- (iv) convertible debt instruments; and
- (v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of section 835.

(f) *Disclosure.* The offeror under this solicitation represents that [Check one]:

it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of Clause)

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

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

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

(a) *Provisions.*

- 3052.209-72 Organizational Conflicts of Interest.
- 3052.216-70 Evaluation of Offers Subject to An Economic Price Adjustment Clause.
- 3052.219-72 Evaluation of Prime Contractor Participation in the DHS Mentor Protégé Program.

(b) *Clauses.*

- 3052.203-70 Instructions for Contractor Disclosure of Violations.
- 3052.204-70 Security Requirements for Unclassified Information Technology Resources.
- 3052.204-71 Contractor Employee Access.
- Alternate I
- 3052.205-70 Advertisement, Publicizing Awards, and Releases.
- 3052.209-73 Limitation on Future Contracting.

- 3052.215-70 Key Personnel or Facilities.
- 3052.216-71 Determination of Award Fee.
- 3052.216-72 Performance Evaluation Plan.
- 3052.216-73 Distribution of Award Fee.
- 3052.219-70 Small Business Subcontracting Plan Reporting.
- 3052.219-71 DHS Mentor Protégé Program.
- 3052.228-70 Insurance.
- 3052.236-70 Special Provisions for Work at Operating Airports.
- 3052.242-72 Contracting Officer's Technical Representative.
- 3052.247-70 F.o.B. Origin Information.
- Alternate I
- Alternate II
- 3052.247-71 F.o.B. Origin Only.
- 3052.247-72 F.o.B. Destination Only.

(End of clause)

#### **I.9 TERM OF CONTRACT (MARCH 2003)**

The term of this contract is from 1/1/2015 through 12/31/2015.

[End of Clause]

#### **I.10 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.11 PAYMENT AND INVOICE INSTRUCTIONS (APR 2014)**

In order to request contract payment, the contractor shall submit a proper invoice, as defined by Federal Acquisition Regulation (FAR) 2.101 for payment in the manner and format described below.

##### **SUBMISSION OF INVOICES**

- (a) The contractor shall submit an original invoice/voucher, via postal mail or electronic mail (email), simultaneously to the following:
  - (1) U.S. Customs and Border Protection  
Commercial Accounts Section

6650 Telecom Drive, Suite 100  
Indianapolis, Indiana 46278

**OR** email: cbpinvoices@dhs.gov

**NOTE:** For invoices with payment terms less than net 30, the subject line for all emailed invoices must include the following text: "**Per CBP, Net [state # days] Invoice**".

(2) Contracting Officer or Contract Administrator (CO or CA) *[fill in at time of award]*

DHS/U.S. Customs and Border Protection  
Attention: (b) (6)

**OR** email: (b) (6)

(3) Contracting Officer's Representative (COR) *[fill in at time of award]*

DHS/U.S. Customs and Border Protection  
Attention: (b) (6)

**OR** email: (b) (6)

- (b) The contractor shall submit a copy of the original invoice/voucher for all DHS cost-reimbursement and time and material/labor hour contracts and delivery orders to the branch manager/resident auditor of the cognizant Defense Contract Audit Agency (DCAA) Field Audit Office. Copies may be sent to DCAA, via postal mail or email and must be sent at the same time the invoice/voucher is sent to the NFC, CO and COR. The CO shall provide the following information:

DCAA Field Office  
Attention:

Phone:

Email:

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

### INVOICE REVIEW AND APPROVAL REQUIREMENTS

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

(1) The minimum requirements are:

- i. Name and address of the contractor.
- ii. Invoice date and invoice number.
- iii. Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).
- iv. Description, quantity, unit of measure, unit price, and extended price of supplies delivered or services performed.
- v. Shipping and payment terms (e.g. shipment number and date of shipment, discount for prompt payment terms). Bill of lading number and weight of shipment will be shown for shipments on Government bills of lading.
- vi. Name and address of contractor official to whom payment is to be sent (must be the same as that in the contract or in a proper notice of assignment).
- vii. Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
- viii. Taxpayer identification number (TIN).

- ix. Electronic funds transfer (EFT) banking information.
  - x. Any other information or documentation required by the contract (e.g. evidence of shipment).
- (2) For cost reimbursement or time and material contracts (other than a contract for a commercial item), the contractor shall bill and maintain a record of indirect costs in accordance with FAR 52.216-7(d).
- (b) Supplemental documentation required for review and approval of invoices, at the written direction of the contracting officer, may be submitted directly to either the contracting officer, or the contracting officer's representative. Contractors shall submit all supplemental invoice documentation along with the original invoice.
- (c) Invoices that fail to provide the information required by the Prompt Payment clause (FAR 52.232-25) may be rejected by the Government and returned to the contractor.

#### **ADDITIONAL INVOICE REQUIREMENTS**

In addition to the invoice requirements contained in FAR 32.905 and FAR 52.216-7, the following also applies:

- (1) Invoices must include the following information to support all costs claimed:
- i. Period of performance for the costs claimed;
  - ii. Current amounts for each CLIN, if applicable;
  - iii. Current direct and indirect incurred costs, including fee;
  - iv. Cumulative amounts for each CLIN; and
  - v. Statement signed by an authorized company representative certifying that the costs in the invoice are accurate and complete.
- (2) The Government reserves the right to make invoice adjustments if associated costs are determined to be unallowable.

[End of Clause]

#### **I.12 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.13 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.14 POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE (JUL 2010)**

**a. Contractor Performance Evaluation**

Interim and final performance evaluation reports will be prepared on this contract or order in accordance with FAR Subpart 42.15. A final performance evaluation report will be prepared at the time the work under this contract or order is completed. In addition to the final performance evaluation report, an interim performance evaluation report will be prepared annually to coincide with the anniversary date of the contract or order.

Interim and final performance evaluation reports will be provided to the contractor via the Contractor Performance Assessment Reporting System (CPARS) after completion of the evaluation. The CPARS Assessing Official Representatives (AORs) will provide input for interim and final contractor performance evaluations. The AORs may be Contracting Officer's Technical Representatives (COTRs), project managers, and/or contract specialists. The CPARS Assessing Officials (AOs) are the contracting officers (CO) who will sign the evaluation report and forward it to the contractor representative via CPARS for comments.

The contractor representative is responsible for reviewing and commenting on proposed ratings and remarks for all evaluations forwarded by the AO. After review, the contractor representative will return the evaluation to the AO via CPARS.

The contractor representative will be given a minimum of thirty (30) days to submit written comments or a rebuttal statement. Within seven (7) days of the comment period, the contractor representative may request a meeting with the AO to discuss the evaluation report. The AO may complete the evaluation without the contractor representative's comments if none are provided within the thirty (30) day comment period. Any disagreement between the AO/CO and the contractor representative regarding the performance evaluation report will be referred to the CPARS Reviewing Officials (ROs). Once the RO completes the review, the evaluation is considered complete and the decision is final. Copies of the evaluations, contractor responses, and review comments, if any, will be retained as part of the contract file and may be used in future award decisions.

b. Primary and Alternate Corporate Senior Contractor Representatives

The contractor must identify a primary and alternate Corporate Senior Contractor Representative for this contract and provide the full name, title, phone number, email address, and business address to the CO within 30 days after award.

c. Electronic access to contractor Performance Evaluations

The AO/CO will request CPARS user access for the contractor by forwarding the contractor's primary and alternate representatives' information to the CPARS Focal Point (FP).

The FP is responsible for CPARS access authorizations for Government and contractor personnel. The FP will set up the user accounts and will create system access to CPARS.

The CPARS application will send an automatic notification to users when CPARS access is granted. In addition, contractor representatives will receive an automated email from CPARS when an evaluation report has been completed.

[End of Clause]

# ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 4

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

1. DATE OF ORDER 09/30/2009	2. CONTRACT NO. (if any) HSHQDC07D00030	6. SHIP TO:			
3. ORDER NO. HSBP1109J28871		4. REQUISITION/REFERENCE NO. 0020045201		a. NAME OF CONSIGNEE  See Attached Delivery Schedule	
5. ISSUING OFFICE (Address correspondence to) CBP, Procurement Directorate ATT: (b) (6) Intech Two, Suite 100 6650 Telecom Drive Indianapolis IN 46278				b. STREET ADDRESS	
7. TO:			c. CITY	d. STATE	e. ZIP CODE
a. NAME OF CONTRACTOR ST NET-APTIS FIRSTSOURCE JOINT				f. SHIP VIA	
b. COMPANY NAME  ATTN: (b) (6)				8. TYPE OF ORDER	
c. STREET ADDRESS 4800 WESTFIELDS BLVD VENTURE				<input type="checkbox"/> 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.	
d. CITY CHANTILLY	e. STATE VA	f. ZIP CODE 20151-2293		<input checked="" type="checkbox"/> 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  CONTRACTOR TIN: (b)(3); (b)(4)				10. REQUISITIONING OFFICE  (b) (6)	
12. F.O.B. POINT Destination		11. BUSINESS CLASSIFICATION (Check appropriate box(es))			
13. PLACE OF		14. GOVERNMENT B/L NO.		15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 09/29/2010	
a. INSPECTION Destination	b. ACCEPTANCE Destination			16. DISCOUNT TERMS  NET 30	

**17. SCHEDULE (See reverse for Rejections)**

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QTY Acpt (g)
00020	AFI support - Lexis/Nexis	1.00	AU	<b>(b) (4)</b>		
00030	XML Set-up Fee - AFI L/N	1.00	AU			
00040	(b) (7)(E) - AFI L/N	1.00	AU			
00060	(b) (7)(E) - AFI L/N	1.00	AU			
00070	(b) (7)(E) - AFI L/N	1.00	AU			
00080	AFI support - Lexis/Nexis_Split Fundg	1.00	AU			

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		17(h) TOT. (Cont. pages)	
21. MAIL INVOICE TO:					
SEE BILLING INSTRUCTIONS ON REVERSE	a. NAME DHS - Customs & Border Protection		National Finance Center		\$0.00
	b. STREET ADDRESS (or P.O. Box) P.O. Box 68908				17(i) GRAND TOTAL
	c. CITY Indianapolis	d. STATE IN	e. ZIP CODE 46268		

22. UNITED STATES  BY (Signature) (b) (6)	23. NAME (Typed) Bruce D. Wood TITLE: CONTRACTING/ORDERING OFFICER
---	--

AUTHORIZED FOR LOCAL REPRODUCTION  
Previous edition not usable

**OPTIONAL FORM 347 (REV. 4/2006)**  
Prescribed by GSA/FAR 48 CFR 53.213 (f)

DATE OF ORDER 09/30/2009	CONTRACT NO. (if any) HSHQDC07D00030	ORDER NO. HSBP1109J28871	PAGE OF PAGES 2 4
-----------------------------	---	-----------------------------	----------------------

**Federal Tax Exempt ID: 72-0408780**

**Emailing Invoices to CBP.** As an alternative to mailing invoices to the National Finance Center as shown on page one of this award, you may email invoices to: **cbpinvoices@dhs.gov**.

**NOTES:**

The vendor shall complete all work in accordance with the attached statement of work (24 pages) and bill of materials (1 page).

The vendor's quotation from 29 Sep 2009, posted via FedBid, is hereby incorporated by refeContent-type: application/vnd.fdf rence.

For contractual questions please contact:

(b) (6)

Contract Specialist

(b) (6)

For technical questions please contact:

(b) (6)

Director, Program Control  
Targeting & Analysis Systems Program Office  
Office of Information & Technology  
Customs & Border Protection  
5971 Kingstowne Village Parkway  
5th Floor Mailroom  
Alexandria, VA 22315

(b) (6) (office)

571-468-1478 (fax)

(b) (6)

ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA  
 FOR DELIVERY ORDER:  
HSBP1109J28871

SCHEDULE OF SUPPLIES/SERVICES

Item Number: 00020 Line Item (Priced/Information/Option): Priced (Labor Hour CLIN)

Supplies/Services: AFI support – LexisNexis-S2.c Support Services

Qty	Unit	Unit Price	Ext. Price
1	AU	(b) (4)	(b) (4)

Item Number: 00030 Line Item (Priced/Information/Option): Priced (Firm Fixed Price CLIN)

Supplies/Services: AFI L/N – LexisNexis-S1.a XML Set-up Fee

Qty	Unit	Unit Price	Ext. Price
1	AU	(b) (4)	(b) (4)

Item Number: 00040 Line Item (Priced/Information/Option): Priced (Firm Fixed Price CLIN)

Supplies/Services: AFI L/N – LexisNexis-S1.b (b) (7)(E)

Qty	Unit	Unit Price	Ext. Price
1	AU	(b) (4)	(b) (4)

Item Number: 00060 Line Item (Priced/Information/Option): Priced (Firm Fixed Price CLIN)

Supplies/Services: AFI L/N – LexisNexis-S1.c (b) (7)(E)

Qty	Unit	Unit Price	Ext. Price
1	AU	(b) (4)	(b) (4)

Item Number: 00070 Line Item (Priced/Information/Option): Priced (Firm Fixed Price CLIN)

Supplies/Services: AFI L/N – LexisNexis-S.1d (b) (7)(E)

Qty	Unit	Unit Price	Ext. Price
1	AU	(b) (4)	(b) (4)

Item Number: 00080 Line Item (Priced/Information/Option): Priced (Labor Hour CLIN)

Supplies/Services: AFI support – LexisNexis-S2.c Support Services (split funding)

Qty	Unit	Unit Price	Ext. Price
1	AU	(b) (4)	(b) (4)

Total Funded Contract Value: \$637,204.12

---

ACCOUNTING AND APPROPRIATION INFORMATION

Item: 00020	6100.2525USCSGLCS0925030400Z00009400HQ01 400022525	Amount	(b) (4)
Item: 00030	6100.2525USCSGLCS0925030400Z00009400HQ01 400022525	Amount	
Item: 00040	6100.2525USCSGLCS0925030400Z00009400HQ01 400022525	Amount	
Item: 00060	6100.2525USCSGLCS0925030400Z00009400HQ01 400022525	Amount	
Item: 00070	6100.2525USCSGLCS0925030400Z00009400HQ01 400022525	Amount	
Item: 00080	6100.2525USCSGLCS0925030400Z00009448AP01 400012525	Amount	

---

DELIVERY SCHEDULE

Deliver To: Customs and Border Protection  
 5971 Kingstown Village Parkway  
 One Kingstown Town Center  
 Alexandria VA 22315

Instructions:					
Item	Quantity	Period of Performance	Recipient	Unloading PT.	
00020	1	09/30/2009 - 09/29/2010	(b) (6)	see address above	
00030	1	09/30/2009 - 09/29/2010		see address above	
00040	1	09/30/2009 - 09/29/2010		see address above	
00060	1	09/30/2009 - 09/29/2010		see address above	
00070	1	09/30/2009 - 09/29/2010		see address above	
00080	1	09/30/2009 - 09/29/2010		see address above	

**Department of Homeland Security  
Customs & Border Protection (CBP)  
Targeting and Analysis Systems Program Office**

**Statement of Work (SOW)**

**1.0 OVERVIEW AND BACKGROUND**

The mission of The Department of Homeland Security (DHS) is to lead the unified national effort to secure America. DHS prevents and deters terrorist attacks and protects against and responds to threats and hazards to the nation. DHS ensures safe and secure borders, welcomes lawful immigrants and visitors, and promotes the free-flow of commerce.

The purpose of the Analytical Framework for Intelligence (AFI) is to define, design, and implement an information framework to support the ever growing and expanding needs of analysis of intelligence data across various network domains. AFI will be a suite of analytical software applications and infrastructure tools integrated into a single powerful platform that will allow intelligence analysts to visualize and analyze large amount of data from disparate data sources utilizing existing and future hardware and software. AFI will host or provide easy access to classified and non-classified data currently located on various systems from different sources and government agencies, and will provide the backbone to achieve the goal of minimizing time spent on data collection and maximize the time spent on analysis.

The planned functionality of AFI will be to integrate “best in breed” GOTS/COTS applications and reuse existing software components to:

- Provide a data consolidation and research platform
- Provide an analysis platform
- Provide a production management platform
- Provide a collaboration and reporting platform

**2.0 OBJECTIVES**

In support of the AFI project, Customs and Border Protection (CBP) will implement solutions to enable CBP to begin to significantly upgrade data management capabilities by obtaining commercially available subscription based data as an XML data feeds. These XML data feeds are feed designed to support the screening, targeting, and tracking of persons that are currently or have been in the United States or are tied to entities within the United States.

**3.0 SCOPE OF WORK**

CBP expects the vendor to deliver the data feeds described in Section 4.0 in an XML format when requested by the AFI application:



#### **4.0 DELIVERABLES**

<b>Item No.</b>	<b>Description</b>
001	Landline Data (LexisNexis) - (b) (7)(E) up to 13,000- Period of Performance 1/1/2013 to 12/31/2013 -XML Feed
002	(b) (7)(E) - 4,000 per month - Period of Performance 1/1/2013 to 12/31/2013-XML Feed
003	(b) (7)(E) - 13,000 per month - Period of Performance 1/1/2013 to 12/31/2013-XML Feed
004	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013-XML Feed
005	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013-XML Feed
006	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013-XML Feed
007	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013-XML Feed
008	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013-XML Feed
009	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013-XML Feed

#### **PERIOD OF PERFORMANCE, LOCATION AND HOURS OF PERFORMANCE**

Period of Performance: 1/1/2013-12/31/2013

Location:

US Customs & Border Protection  
Targeting and Analysis Systems Program Office  
5971 Kingstowne Village Parkway  
Fifth Floor Mailroom  
Alexandria, VA 22315

And contractor facilities.

#### **4.0 INVOICING AND PAYMENT**

The contractor shall submit one invoice for the hardware cost. Invoices shall be electronically transmitted to the Technical Point of Contact listed in section 5.0. To constitute a proper invoice, each invoice shall be annotated with at least the following information:

- Order number
- Description of services provided for a specified time period.
- Unit price and total amount of each item.
- Discount terms
- Company name, telephone number, taxpayer's identification number, and complete mailing address to which payment will be mailed.

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

## **5.0 POINT OF CONTACT**

### CONTRACTING OFFICER'S REPRESENTATIVE

(b) (6)

Customs & Border Protection  
Office of Information & Technology  
Targeting and Analysis Systems Program Office  
5971 Kingstowne Village Parkway  
Fifth Floor Mailroom  
Alexandria, VA 22315

Office phone: (b) (6)

e-mail: (b) (6)

## **6.0 DHS Clauses**

### **Enterprise Architecture (EA) Compliance**

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

The Offeror shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model as described in their respective EAs. Models will be submitted using Business Process Modeling Notation (BPMN) version 2.0 and the CBP Architectural Modeling Standards for all models. Universal Modeling Language (UML2) may be used for infrastructure only. Data exchange formats and semantics shall be in conformance with the

National Information Exchange Model (NIEM), version 2.0. Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

The contractor shall maintain close coordination with the CBP Enterprise Architecture Branch (EAB) and utilize the Central Enterprise Architecture Repository (CEAR), for capturing performance measures, business processes, application designs, technical infrastructure designs, and other related designs for the project. The contractor shall develop performance indicators and ensure appropriate mapping to the Performance Reference Model (PRM); develop business process flows and ensure appropriate mapping to CBP Lines of Business and Business Reference Model (BRM); develop application models capturing system components, subsystems, and information exchanges between system in development and other systems and ensure appropriate mapping of the system under development to Service Component Reference Model (SRM) and the Technical Reference Model (TRM); develop data models and data exchanges that align to the Data Reference Model (DRM) and develop models of technical infrastructure that will be used to support the systems under development.

All IT hardware and software shall comply with the DHS and CBP Technical Reference Models (TRM). The Offeror shall use DHS/CBP approved products, standards, services, and profiles as reflected by the hardware software, application, and infrastructure components of the DHS/CBP TRM/Standards Profile. If new hardware, software and infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal technology insertion process which includes a trade study with no less than four alternatives, one of which shall reflect the status quo and one shall reflect multi-agency collaboration. The DHS/CBP TRM/Standards Profile will be updated as technology insertions are accomplished.

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

All developed solutions shall be compliant with the HLS and CBP EA. Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

In compliance with Office of Management and Budget (OMB) mandates, all network hardware provided under the scope of this Statement of Work and

associated Task Orders (TO) shall be IPv6 compatible without modification, upgrade, or replacement.

## **OAST (Office on Accessible Systems and Technology) Compliance**

- **DHS Accessibility Requirements Tool (DART)**

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to [accessibility@dhs.gov](mailto:accessibility@dhs.gov).

### **Accessibility Requirements (Section 508)**

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

### **Section 508 Applicable EIT Accessibility Standards**

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

### **Section 508 Applicable Exceptions**

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

### **Section 508 Compliance Requirements**

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under

an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

### **EBMO (Investment Review) Compliance**

- Legitimate Investments must be identified (on line 15 of the DHS Checklist) - based on Exhibit 53 (attached). Also, if more than 1 investment is identified – please split out the cost associated with each investment.

### **ISO (Information Security) COMPLIANCE**

- **Information Security Clause**

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

- **Interconnection Security Agreements**

Interconnections between DHS and non-DHS IT systems shall be established through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements. Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have signatory authority.

- **HSAR Clauses**

#### **3052.204-70 Security Requirements For Unclassified Information Technology Resources (JUN 2006)**

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the

Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 15 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the

contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 8.0, March 14, 2011) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

## **HSAR 3052.204-71 Contractor Employee Access Clause**

### **CONTRACTOR EMPLOYEE ACCESS (JUN 2006)**

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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



(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO)

and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

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

Security Certification/Accreditation

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

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

### **Disaster Recovery Planning & Testing – Hardware (if applicable)**

If the system owner requires a robust DR solution (full redundancy and failover capabilities (for near zero downtime)) then the funded DR solution must match the production environment like-for-like. This solution would also include additional software licenses, hardware, firmware and storage for the DR environment.

The system owner or program office must also include travel, per diem and approximately 16 over the core hours for travel to recovery facilities twice per fiscal year for system administrators, DBA's, end users or testers

If the system owner requires a moderate DR solution that would provide a working environment that is capable of handling their mission essential functions then they can fund a scaled down solution which should still take into consideration additional hardware, software licenses, and storage for the DR environment.

The system owner or program office is still responsible for the costs associated with testing their DR solution; however, for a scaled down solution, it may be possible to leverage or share staff already designated to participate in DR activities.

If the system owner only requires a low DR solution then the system owner or program office can use internal resources to perform a table-top exercise, which generally does not require travel, additional hardware or software licenses.

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

#### Security Review and Reporting

(a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.

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

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

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

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

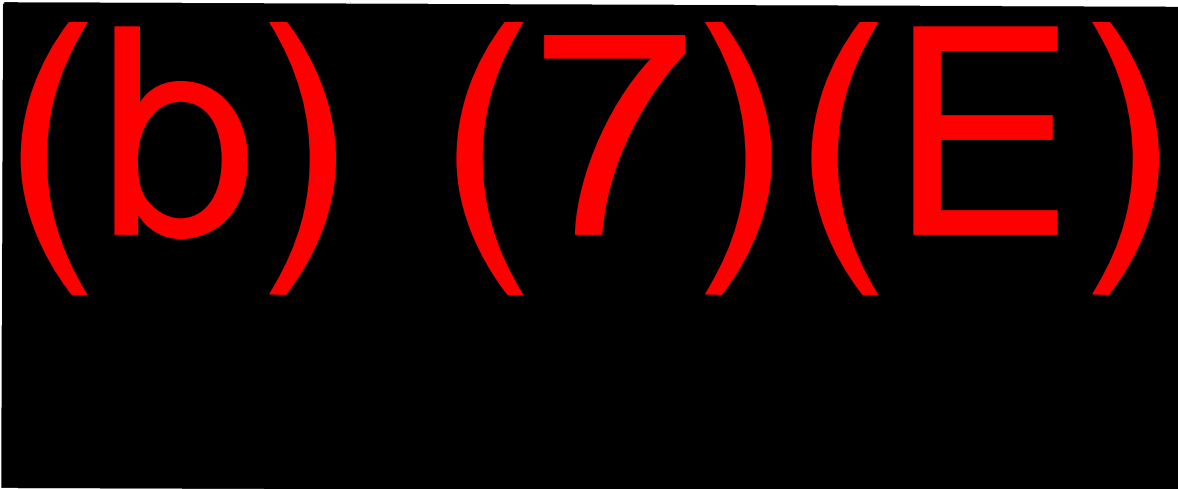
#### **OMB-M-07-18 FDCC**

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

#### **Engineering Platforms**

- **Common Enterprise Services (CES)** – Deliver the systems, infrastructure, and operational capabilities to fully implement the three service levels defined as part of the DHS/CBP Common Enterprise Services and support DHS Component use of those services. This

**(b) (7)(E)**



**ITP (Infrastructure Transformation Program) COMPLIANCE  
(if applicable)**

- **Help Desk and Operations Support**

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

- **Interfacing**

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

**TRANSITION PLAN (if applicable)**

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

- Coordination with Government representatives

- Review, evaluation and transition of current support services
- Transition of historic data to new contractor system
- Government-approved training and certification process
- Transfer of all necessary business and/or technical documentation
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable debriefing and personnel out-processing procedures

## **Portfolio Review**

### **Screening/Watchlist/Credentialing**

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

**Department of Homeland Security  
Customs & Border Protection (CBP)  
Targeting and Analysis Systems Program Directorate**

**Statement of Work (SOW)**

**1.0 OVERVIEW AND BACKGROUND**

The mission of The Department of Homeland Security (DHS) is to lead the unified national effort to secure America. DHS prevents and deters terrorist attacks and protects against and responds to threats and hazards to the nation. DHS ensures safe and secure borders, welcomes lawful immigrants and visitors, and promotes the free-flow of commerce.

The purpose of the Analytical Framework for Intelligence (AFI) is to define, design and implement an information framework to support the ever growing and expanding needs of analysis of intelligence data across various network domains. AFI is a suite of analytical software applications and infrastructure tools integrated into a single powerful platform that allows intelligence analysts to visualize and analyze large amount of data from disparate data sources utilizing existing and future hardware and software.

**2.0 OBJECTIVES**

In support of the AFI project, Customs and Border Protection (CBP) has a need to access commercially available subscription based data as XML data feeds. These XML data feeds are designed to support the screening, targeting, and tracking of persons that are currently or have been in the United States or are tied to entities within the United States.

**3.0 SCOPE OF WORK**

CBP expects the vendor to deliver the data feeds described in Section 4.0 in an XML format when requested by the AFI application for the period of performance.

**4.0 DELIVERABLES**

<b>Item No.</b>	<b>Description</b>
001	(b) (7)(E) up to 13,000 per month- Period of Performance 1/1/2015 to 12/31/2015 –XML Feed
002	(b) (7)(E) – 4,000 per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
003	(b) (7)(E) – 13,000 per month - Period of Performance 1/1/2015 to



	12/31/2015–XML Feed
004	(b) (7)(E) - 1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
005	(b) (7)(E) - 1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
006	(b) (7)(E) - 1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
007	(b) (7)(E) -1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
008	(b) (7)(E) -1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
009	(b) (7)(E) -1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed

**5.0 PERIOD OF PERFORMANCE AND LOCATION**

Period of Performance: January 1, 2015 to December 31, 2015.

Location: Contractor facilities.

**6.0 INVOICING AND PAYMENT**

Invoices shall be electronically transmitted to the Point of Contact listed in section 7.0. To constitute a proper invoice, each invoice shall be annotated with at least the following information:

- Order number
- Description of services provided for a specified time period.
- Unit price and total amount of each item.
- Discount terms
- Company name, telephone number, taxpayer’s identification number, and complete mailing address to which payment will be mailed.

Copies of invoices (paper submissions) will be submitted to the following addresses *OR as an alternative*, to the email addresses cited below:

1. Payment Center:

DHS/U.S. Customs and Border Protection  
National Finance Center/Commercial Accounts  
P. O. Box 68908  
Indianapolis, Indiana 46268

*OR as an alternative:*

Email: [cbpinvoices@dhs.gov](mailto:cbpinvoices@dhs.gov)

2. Contracting Officer's Representative

DHS/U.S. Customs and Border Protection  
Attention: (b) (6)  
5971 Kingstowne Village Pkwy  
5th Floor Mailroom  
Alexandria, VA 22315

Email: (b) (6)

3. Contracting Officer's Representative - Alternate

DHS/U.S. Customs and Border Protection  
Attention: (b) (6)  
5971 Kingstowne Village Pkwy  
5th Floor Mailroom  
Alexandria, VA 22315

Email: (b) (6)

3. TASP Budget POC

DHS/U.S. Customs and Border Protection  
Attention: (b) (6)  
5971 Kingstowne Village Pkwy  
5th Floor Mailroom  
Alexandria, VA 22315

Email: (b) (6)

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

## **7.0 POINT OF CONTACT**

### CONTRACTING OFFICER'S REPRESENTATIVE

(b) (6)

Customs & Border Protection  
Office of Information & Technology  
Targeting and Analysis Systems Program Directorate  
5971 Kingstowne Village Parkway  
Fifth Floor Mailroom  
Alexandria, VA 22315  
Office phone: (b) (6)  
E-mail: (b) (6)

### CONTRACTING OFFICER'S REPRESENTATIVE – ALTERNATE

(b) (6)

Customs & Border Protection  
Office of Information & Technology  
Targeting and Analysis Systems Program Directorate  
5971 Kingstowne Village Parkway  
Fifth Floor Mailroom  
Alexandria, VA 22315  
Office phone: (b) (6)  
E-mail: (b) (6)

## **8.0 Clauses**

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

### **Enterprise Architecture (EA) Compliance**

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

The Offeror shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model, as described in their respective EAs. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be

in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

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

All developed solutions shall be compliant with the Homeland Security (HLS) EA.

All IT hardware and software shall be compliant with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

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

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

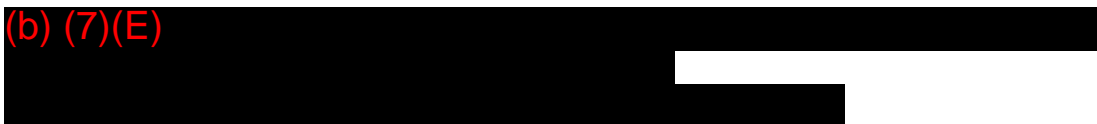
### **Compliance with DHS Security Policy Terms and Conditions**

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

### **Encryption Compliance**

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

(b) (7)(E)

A large black rectangular redaction box covers the majority of the text in this section. The text "(b) (7)(E)" is visible in red at the top left of the redaction.

(b) (7)(E)

**HSAR 3052.204-70 Security Requirements For Unclassified Information  
Technology Resources (JUN 2006)**

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 15 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer.

Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 8.0, March 14, 2011) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting

Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

## **CONTRACTOR EMPLOYEE ACCESS (JUN 2012)**

(a) Sensitive Information, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of S SI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated

background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

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

(3) The waiver must be in the best interest of the Government.

(1) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

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

### **Security Authorization**

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

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

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

### **Enterprise Security Architecture**

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



(b) (7)(E)

5) Performance of activities per continuous monitoring requirements

### **Continuous Monitoring**

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

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

### **Specific Protections**

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

### **Security Operations**

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

### **Computer Incident Response Services**

The Contractor shall provide Computer Incident Response Team (CIRT) services. The contractor shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The contractor shall conduct Incident

Response Exercises to ensure all personnel are familiar with the plan. The contractor shall notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration.

### **Firewall Management and Monitoring**

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

### **Intrusion Detection Systems and Monitoring**

The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. (b) (7)(E)

The NIDS shall operate 24x7x365. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

### **Physical and Information Security and Monitoring**

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

### **Vulnerability Assessments**

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

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

The Contractor shall design, implement, monitor and manage to provide comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COR in weekly

status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

### **Patch Management**

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

### **Log Retention**

Log files for all infrastructure devices, physical access, and anti-malware should be retained (b) (7)(E).

### **Personal Identification Verification (PIV) Credential Compliance**

Authorities:

HSPD-12 —Policies for a Common Identification Standard for Federal Employees and Contractors

OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors"

OMB M-06-16 —Acquisition of Products and Services for Implementation of HSPD-12  
NIST FIPS 201 —Personal Identity Verification (PIV) of Federal Employees and Contractors

NIST SP 800-63 —Electronic Authentication Guideline

OMB M-10-15 —FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

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

Procurements for software products or software developments shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

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

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

## **OAST (Office on Accessible Systems and Technology) Compliance**

### **Accessibility Requirements (Section 508)**

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

### **Section 508 Applicable EIT Accessibility Standards**

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

### **Section 508 Applicable Exceptions**

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

### **Section 508 Compliance Requirements**

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to [accessibility@dhs.gov](mailto:accessibility@dhs.gov).

## **ISO (Information Security) COMPLIANCE**

### **Information Security Clause**

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

### **Interconnection Security Agreements**

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

agreements; memoranda of understanding, service level agreements or interconnect service agreements.

### **System Security documentation appropriate for the SELC status.**

#### Security Certification/Accreditation

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

#### **Disaster Recovery Planning & Testing – Hardware**

If the system owner requires a robust DR solution (full redundancy and failover capabilities (for near zero downtime)) then the funded DR solution must match the production environment like-for-like. This solution would also include additional software licenses, hardware, firmware and storage for the DR environment.

The system owner or program office must also include travel, per diem and approximately 16 over the core hours for travel to recovery facilities twice per fiscal year for system administrators, DBA's, end users or testers

If the system owner requires a moderate DR solution that would provide a working environment that is capable of handling their mission essential functions then they can fund a scaled down solution which should still take into consideration additional hardware, software licenses, and storage for the DR environment.

The system owner or program office is still responsible for the costs associated with testing their DR solution; however, for a scaled down solution, it may be possible to leverage or share staff already designated to participate in DR activities.

If the system owner only requires a low DR solution then the system owner or program office can use internal resources to perform a table-top exercise, which generally does not require travel, additional hardware or software licenses.

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

#### Security Review and Reporting

(a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.

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

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

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

### **OMB-M-07-18 FDCC**

In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's

website at <http://checklists.nist.gov>. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.

### **Engineering Platforms**

**Common Enterprise Services (CES)** – Deliver the systems, infrastructure, and operational capabilities to fully implement the three service levels defined as part of the DHS/CBP Common Enterprise Services and support DHS Component use of those services. (b) (7)(E)

[Redacted]

(b) (7)(E)

[Redacted]

### **ITP (Infrastructure Transformation Program) COMPLIANCE**

#### **Help Desk and Operations Support**

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

#### **Interfacing**

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

#### **TRANSITION PLAN**

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

- Coordination with Government representatives



- Review, evaluation and transition of current support services
- Transition of historic data to new contractor system
- Government-approved training and certification process
- Transfer of all necessary business and/or technical documentation
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable debriefing and personnel out-processing procedures

## **Portfolio Review**

### **Screening/Watchlist/Credentialing**

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

# Analytical Framework for Intelligence Statement of Work

## 1.0 OVERVIEW AND BACKGROUND

The mission of The Department of Homeland Security (DHS) is to lead the unified national effort to secure America. DHS prevents and deters terrorist attacks and protects against and responds to threats and hazards to the nation. DHS ensures safe and secure borders, welcomes lawful immigrants and visitors, and promotes the free-flow of commerce.

The purpose of the Analytical Framework for Intelligence (AFI) is to define, design, and implement an information framework to support the ever growing and expanding needs of analysis of intelligence data across various network domains. AFI will be a suite of analytical software applications and infrastructure tools integrated into a single powerful platform that will allow intelligence analysts to visualize and analyze large amount of data from disparate data sources utilizing existing and future hardware and software. AFI will host or provide easy access to classified and non-classified data currently located on various systems from different sources and government agencies, and will provide the backbone to achieve the goal of minimizing time spent on data collection and maximize the time spent on analysis.

The planned functionality of AFI will be to integrate “best in breed” GOTS/COTS applications and reuse existing software components to:

- Provide a data consolidation and research platform
- Provide an analysis platform
- Provide a production management platform
- Provide a collaboration and reporting platform

## 2.0 OBJECTIVES

In support of the AFI project, Customs and Border Protection (CBP) will implement two solutions to enable CBP to begin to significantly upgrade data management capabilities as follow:

1. The XML Data Feed: An XML data feed designed to support the screening, targeting, and tracking of persons that are currently or have been in the United States or are tied to entities within the United States.
2. The Pilot Entity Resolution System: A prototype implementation of technology and data management services to enable CBP to cleanse existing data repositories and continuously ingest, disambiguate, and correlate the many distinct personnel and trade entities managed by CBP.

### **3.0 SCOPE OF WORK**

CBP estimates approximately 2800 hours of professional services support and consulting for integration. This effort will include, but are not limited to, efforts designed to:

- Ingest the existing data sets at CBP
- Cleanse the disparate data and provide a consistent format
- Provide simple queries to allow for basic access to the refined entities
- Provide very simple entity correlation based on examination of the different fields in the data

### **4.0 DELIVERABLES AND REPORTING REQUIREMENTS**

All deliverables produced as a result of this Statement of Work (SOW) shall become the property of the Government.

Additional, deliverables will be defined in each task order, based on the requirements and objectives associated within the particular task order. Contractor shall provide the following deliverables:

#### **4.1 Timesheets**

Contractor shall provide the Contracting Officer's Technical Representative (COTR) with monthly timesheets for approval and signature. Professional services shall be invoiced monthly for the hours worked. All timecards presented for COTR approval shall be services rendered within the scope of section 3.0 of this SOW.

#### **4.2 Weekly Status Reports**

The Contractor shall provide the COTR with a weekly report, for each task in section 4.0, not to exceed three (3) pages outlining the engagement progress, with an overview of work accomplished the previous period and work scheduled for the upcoming week. These reports will be deemed accepted upon delivery. This report shall contain the following information, which can be changed at the discretion of the COTR:

- A cover letter with the Contractor's name and address, the contract number, the date of the report, name and telephone number of the preparer of the report; and the period covered by the report;
- Description of task during the reporting period;
  1. If applicable, trip reports and significant results;
- Status justification of the task and other work efforts assigned to the Contractor staff, broken out by individual and related to the task or work effort to which they are assigned;
- Accomplishments during the reporting period;

- Issues and Risks areas affecting technical, schedule, or cost elements of the contract, including background, impact and recommendations for resolution;
  1. Results related to previously identified problem areas with conclusions and recommendations;
- Planned activities and desired results for the next reporting period;
- Priority Items and desired results for the next reporting period;
- Task Schedule: Milestones and Deliverables with status.

Contractor Task:				
Description/Title Of Milestone/Deliverable	Original Due Date	Current Due Date	% Complete	Notes

#### 4.3 Contract Cost Report

Contractor shall submit a monthly Contract Cost Report to the COTR. The Contract Cost Report is a summary of all costs associated with the contract, on a Task Order by Task Order basis. Report shall be broken down by Task Order and individual labor categories within Task Orders. It will also include costs for the current fiscal year, as well as total costs to date for the contract.

#### 4.4 Ad Hoc Reports

Contractor shall submit Ad Hoc reports, in DHS' choice of document layout, when requested by the COTR. These Ad Hoc reports can cover, but are not limited to areas as:

- Trip reports;
- Meeting agenda reports;
- Meeting minutes

#### 4.5 Report Formats

All reports shall be delivered in softcopy electronic format. Softcopies shall be delivered utilizing Microsoft Office file formats. Contractor shall submit all reports electronically to the COTR's DHS electronic mail address. In the event the system is unavailable or not accessible due to a system malfunction, Contractor shall submit all reports in a typewritten format to be followed simultaneously with an electronically transmitted copy as soon as the electronic mail system becomes available.

#### 4.6 Reporting Requirements

SOW REFERENCE	REPORT TITLE	DELIVERY DATE
SOW Section 5.0	Weekly Status Report	Close of business every Friday.
SOW Section 5.0	Ad Hoc Reports	As required.

#### 4.7 Deliverables Requirements

SOW REFERENCE	DELIVERABLE TITLE	DELIVERY DATE
SOW Section 5.0	Timesheets	As required per invoice cycle.

### 5.0 ACCEPTANCE CRITERIA

Acceptance will be provided via timesheets. All signed timesheets will constitute approval of hours worked. For general quality measures, as set forth below, the following will be applied to each deliverable or work product received from Contractor under this SOW:

**Accuracy** - Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style. All deliverables shall conform to the appropriate DHS Directive or Office of Management and Budget (OMB) circular.

**Clarity** - Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand and relevant to the supporting narrative.

**Specifications Validity** - All Deliverables shall satisfy the requirements of the Government as specified herein.

**File Editing** - All text and diagrammatic files shall be editable by the Government.

**Timeliness** - Deliverables shall be submitted on or before the due date specified in this task order. The COTR shall be notified prior to the due date in the event that this cannot be met.

### 6.0 GOVERNMENT FURNISHED EQUIPMENT/PROPERTY/MATERIAL

#### 6.1 Government Furnished Equipment

The Government will provide personnel with semi-private work areas equipped with a workstation, and have access to a laser printer, telephones, and general

office supplies. Some work may be performed off-site at Contractor offices. Any off-site work shall be coordinated and approved with the COTR.

Additional Government Furnished Equipment will be defined in each task order.

## 6.2 Government Furnished Information

DHS will provide timely and accurate information as well as access to appropriate DHS resources to Contractor so it can complete the requirements in the task order. Government Furnished Information will be defined in each task order and may include, but not be limited to:

Item / Document
Access to personnel who are knowledgeable in the current DHS IT systems.
Copies of all test cases, test data, DHS-specific procedures, and personnel required to conduct acceptance testing of the solution.
Necessary work site access, to include necessary DHS system log-ins and passwords.
Access to proper licenses to all necessary tools and third party products required for Contractor to complete the assigned the tasks.
Access to regular system backups.

## 7.0 PLACE OF PERFORMANCE

The Government will provide access to appropriate resources, including, but not limited to: related employees/ vendors/ developers/ consultants, appropriate work space, hardware, software, network connections, test and live data. Support of this task may also require travel to various DHS locations throughout the United States, such as to conduct pilots.

Work will be performed at the CBP OIT office at 5971 Kingstowne Village Parkway, Alexandria, VA 22315. However this site may change during task order performance.

## 8.0 TRAVEL

All travel shall be in accordance with the Federal Travel Regulations (for travel in 48 contiguous states), the Joint Travel Regulations, Department of Defense (DoD) Civilian Personnel, Volume 2, Appendix A (for travel to Alaska, Hawaii, Puerto Rico, and U.S. territories and possessions), and, if applicable, the Standardized Regulations (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" (for travel not covered in the Federal Travel Regulations or Joint Travel Regulations).

Contractor shall be reimbursed for actual travel expenses incurred based on the fixed travel per diem rates and mileage rate for travel commencing or terminating outside of the assigned duty station.

Contractor shall be responsible for travel arrangements for Contractor personnel as defined in each task order. This includes travel, subsistence, and associated labor charges for travel time. Travel performed for personal convenience and daily travel to and from work at a Contractor facility will not be reimbursed.

No travel will be reimbursed without prior written approval from the task order COTR. A not-to-exceed amount may be included in the task order to cover estimated travel expenses.

## **9.0 OTHER DIRECT COSTS**

There are no Other Direct Costs, other than travel as described in Section 8.0, anticipated under this SOW.

## **10.0 SECURITY**

Contractor shall comply with the DHS administrative, physical, and technical security controls to ensure that the Government's security requirements are met. During the course of this task order, Contractor shall not use, disclose, or reproduce data, which bears a restrictive legend, other than as required in the performance of this SOW. All contractors working under this SOW will be required to attain and retain a TS/SCI clearance.

All personnel employed by Contractor and/or responsible to Contractor for work performed hereunder shall either currently possess or be able to successfully pass a background investigation. This policy applies to any new personnel hired as replacement(s) during the term of this task order.

Contractor shall submit within two (2) weeks after award:

A list containing the full name, social security number, and date of birth of those people who will require background investigation by DHS and, submit such information and documentation as may be required by the Government to have a background investigation performed.

The information must be correct and reviewed by the designated DHS Security Official for completeness. Normally, information requested for a background investigation consists of SF-85P, "Questionnaire for Public Trust Positions" or SF-86, "Questionnaire for Sensitive Positions (For National Security)" TDF 67-32.5, "U.S. USCS Authorization for Release of Information", FD-258, "Fingerprint Chart" and a Financial Statement. Failure of any contract personnel to successfully pass a background investigation shall be cause for the candidate's dismissal from the project and replacement by a similar and equally qualified candidate as determined and approved by the Contracting Officer (CO)/COTR.

This policy also applies to any personnel hired as replacements during the term of the SOW.

Upon award and when applicable, the DHS assigned COTR of record shall be responsible for processing the "Department of Defense, Contract Security Classification Specification (DD254)" on behalf of the Contractor. The DD254 will authorize the Contractor to conduct additional background investigations for assigned contract personnel required to access SCI facilities and/or classified National Security information and applies to any and all personnel hired as replacements during the term of the task order.

Contractor shall immediately notify the CO and COTR of any personnel changes. Written approval and confirmation is required for phone notification. This includes, but is not limited to, resignations, terminations, and reassignments.

In accordance with Customs Directive No. 51715-006, "Separation Procedures for Contractor Employees (CF-242)" Contractor is responsible for ensuring that contract employees separating from the agency complete the relevant portions of the CF-242. This requirement covers all contract employees who depart while the SOW is still active (including resignation, termination, etc.) or upon final completion of this SOW. Failure of a contractor to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports.

Contractor shall notify the COTR and DHS OE Security Contractor/Engagement Manager of any changes in access requirements for its personnel no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to another contract. The Contractor/Engagement Manager is responsible for the completion and timely submission to the COTR of the CF-242 for all departing contract personnel. Contractor personnel must provide:

- Full Name
- Social Security Number
- Effective Date
- Reason for Change

Contractor employees shall be required to wear DHS identification badges at all times when working in Government facilities.

All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures.

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



## **11.0 PERIOD OF PERFORMANCE, ESTIMATED STAFFING REQUIREMENTS AND LABOR CATEGORIES**

The period of performance for this SOW is one (1) year from date of award.

## **12.0 PERSONNEL AND WORK HOURS**

Contractor shall typically work 8 hours a day, 5 days a week, but may be required to work beyond this typical schedule. Contractor personnel shall observe a consistent tour of duty of 40 hours per week, Monday through Friday, with core hours from 9:30 AM until 3:30 PM; any alterations to the work schedule shall be negotiated with the COTR. Contractor personnel shall be available for weekend and after hours work as directed by the COTR and may be called upon for after-hours emergencies. All Contractor personnel shall be present during core hours and have an appropriate set of skill sets to support the services in this SOW from 8:00 AM to 5:00 PM.

Contractor personnel may not work more than 40 hours a week without prior approval from the COTR. Approved overtime hours shall be invoiced at the normal hourly rate.

Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance and integrity and shall be responsible for their employee's performance or the quality of their services.

DHS personnel observe the following days as holidays:

New Year's Day,	Labor Day
Martin Luther King's Birthday,	Columbus Day
Presidents' Day,	Veterans Day
Memorial Day,	Thanksgiving Day
Independence Day,	Christmas Day

Any other day designated by Federal statute, by Executive Order or by the President's proclamation.

When any such day falls on a Saturday the preceding Friday is observed. When any such day falls on a Sunday, the following Monday is observed. Observance of such days by Government personnel shall not be cause for an extension to the delivery schedule or period of performance or adjustment to the price, except as set forth in the contract.

Except for designated around-the-clock or emergency operations, contractor personnel will not, without written consent from the COTR, be able to perform on site under this task order with DHS on the holidays set forth above. Contractor will not charge any holiday as a direct charge to the contract. In the event that Contractor personnel work during a holiday other than those above, no form of holiday or other premium compensation will be reimbursed as either a direct or indirect cost. However, this does not preclude reimbursement for authorized overtime work.

In the event DHS grants administrative leave to its Government employees, at the site, on-site Contractor personnel shall also be dismissed if the site/facility is being closed, however, Contractor shall continue to provide sufficient personnel to perform around-the-clock requirements of critical efforts already in progress or scheduled and shall be guided by the instructions issued by the CO or her/his duly appointed representative. In each instance when the site is closed to Contractor personnel as a result of inclement weather, potentially hazardous conditions, explosions, or other special circumstances: Contractor shall direct its staff as necessary to take actions such as reporting to its own site(s) or taking appropriate leave consistent with its policies. The cost of salaries and wages to Contractor for the period of any such site closure are a reimbursable item of direct cost under the contract for employees whose regular time is normally a direct charge if they continue to perform SOW work; otherwise, costs incurred because of site closure are reimbursable as indirect costs in accordance with Contractor's established accounting policy.

Work may only be performed on a Federal holiday and/or at Contractor's site with written consent of the COTR.

Contractor shall ensure that its employees will identify themselves as employees of their respective company while working on DHS contracts. For example, Contractor personnel shall introduce themselves and sign attendance logs as employees of their respective companies, not as DHS employees.

Contractor shall ensure that their personnel use the following format signature on all official e-mails generated by DHS computers:

[Name]  
[Position or Professional Title]  
[Company Name]  
Supporting the XXX Division/Office...  
Bureau of Customs and Border Protection  
[Phone]  
[FAX]  
[Other contract information as desired]

### **13.0 INVOICE REQUIREMENTS**

Monthly invoices shall be submitted for all costs accrued during the monthly reporting period. The monthly reporting period may be a calendar month or any other period used by Contractor as a billing cycle, provided that this billing cycle has no fewer than 28 and no more than 31 days in it.

Invoices shall separately identify costs for each task order or modification. Invoices shall include copies of all contractor time sheets. Time sheets shall be submitted to the COTR prior to invoicing, but must be submitted no later than accompanying the relevant invoice. Invoices will be rejected if not supported by Contractor time sheets.

Invoices for the cost of any subcontractor shall be submitted separately if there is any delayed billing for the hours worked by the subcontractor. Invoices for subcontractor hours shall reflect the actual dates the subcontractors performed their work and shall not be consolidated into Contractor's invoices with differing periods of performance.

Invoices shall be submitted either in hard copy or electronically by email to the COTR, who will be identified in the individual Task Orders.

Copies of time sheets should be submitted to the COTR with the invoices. If available, time sheets should be submitted electronically. If not available electronically, hard copies of the time sheets must be submitted to arrive no later than receipt of the invoice.

Invoices shall be submitted within ten (10) working days of the end of Contractor's accounting cycle.

Invoices shall contain:

- Company name and address.
- Name and address of person to whom payment is to be sent, including EFT information, if applicable.
- Name, title, and phone number of person to notify in the event of defective invoices.
- The period being invoiced. This must include the beginning and end dates (dd/mm/yyyy format) of the calendar month or billing cycle period being invoiced.
- Contract Number.
- Task Order Number (or Task Order Modification Number).
- Total Value of Task Order (or Task Order Modification Value).
- Task Order Period of Performance.
- Monthly Tabulation as follows:

1. Monthly hours by labor category, and, broken out within each labor category, monthly hours by individual employee.
  2. Labor Category Rates.
  3. Total cost by labor category and by individual employee.
- Summary Tabulation as follows:
    1. Summary hours, to date, by labor category.
    2. Labor Category Rate.
    3. Total cost, to date, by labor category.

Certification by a competent company official that the invoice contains all accrued costs for the month to the best of the official's knowledge.

#### **14.0 NON-DISCLOSURE OF INFORMATION**

Any information made available to Contractor by DHS shall be used only for the purpose of performing the required task and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the task. Contractor employees will be required to sign Non-Disclosure statements.

#### **15.0 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE**

Ms. (b) (6)  
Customs & Border Protection  
Office of Information & Technology  
Targeting & Analysis Systems Program Office  
5971 Kingstowne Village Parkway  
5th Floor Mailroom  
Alexandria, Virginia 22315  
Office phone-(b) (6)  
Office fax-571-468-1477  
e-mail-(b) (6)

#### **16.0 DHS clauses**

Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998, requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to and use of information and services that is comparable to the access and use available to non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following standards and have been identified:

- 36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.
- 36 CFR 1194.22 – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as Flash or Asynchronous Javascript and XML (AJAX) then “1194.21 Software” standards apply to fulfill functional performance criteria.
- 36 CFR 1194.23 – Telecommunications Products. This applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured or developed when the item will be used by member(s) of the public or Federal employee(s).
- 36 CFR 1194.24 – Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.
- 36 CFR 1194.25 – Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement. Specifically but not limited to items using biometrics as described in this work order shall apply with this requirement as well as any other technical standard involving the use of software or Web based interfaces.
- 36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.
- 36 CFR 1194.31 – Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use

technical standards, regardless of technology, to fulfill the functional performance criteria.

- 36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required “1194.31 Functional Performance Criteria”, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this work statement have been determined by DHS. Only the exceptions described herein shall be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may be applied:

36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards.

When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires approval from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

- 36 CFR 1194.3(b) – Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

- 36 CFR 1194.3(f) – Back Office, applies to any EIT item that will be located in spaces frequented only by service personnel for maintenance, repair,

or occasional monitoring of equipment. This exception does not include remote user interfaces that are accessible outside the enclosed “space”.

## **EA (Enterprise Architecture) Compliance**

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

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

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles as reflected by the hardware software, application, and infrastructure components of the DHS/CBP TRM/Standards Profile. If new hardware, software and infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal technology insertion process which includes a trade study with no less than four alternatives, one of which shall reflect the status quo and one shall reflect multi-agency collaboration. The DHS/CBP TRM/Standards Profile will be updated as technology insertions are accomplished.

All developed solutions shall be compliant with the HLS (Homeland Security) EA (Enterprise Architecture) and the CBP EA.

All IT hardware or software shall comply with the HLS EA and the CBP EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model. Submittal shall be through the CBP Data Engineering Branch and CBP EA.

In compliance with OMB mandates, all network hardware provided under the scope of this Statement of Work and associated Task Orders shall be IPv6 compatible without modification, upgrade, or replacement.

## **EBMO (Investment Review) Compliance**

- Legitimate Investments must be identified (on line 15 of the DHS Checklist) - based on Exhibit 53 (attached). Also, if more than 1 investment is identified – please split out the cost associated with each investment.

- **Interconnection Security Agreements**

Interconnections between DHS and non-DHS IT systems shall be established through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements. Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have signatory authority.

- HSAR Clauses

3052.204-70 Security Requirements for Unclassified Information Technology Resources (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and



procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 15 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

### **3052.204-71 Contractor employee access.**

As prescribed in (HSAR) 48 CFR [3004.470-3\(b\)](#), insert a clause substantially the same as follows with appropriate alternates:

#### **CONTRACTOR EMPLOYEE ACCESS (JUN 2006)**

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

When the contract will require contractor employees to have access to Information Technology (IT) resources:

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of

Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

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

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

When the Department has determined contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to IT resources:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-55 1). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

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

Security Certification/Accreditation

DHS shall provide personnel with the appropriate clearance levels to support the security certification/accreditation processes under this

Agreement in accordance with DHS MD 4300A, DHS Sensitive Systems Policy and Handbook. During all SDLC phases of DHS systems, DHS personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools.

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

Security Review and Reporting

(a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.

(b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the Office of Inspector General, CBP CISO, and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/CBP data or the function of computer systems operated on behalf of DHS/CBP, and to preserve evidence of computer crime.

Engineering Platforms

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

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

## **ITP (Infrastructure Transformation Program) COMPLIANCE**

- **Help Desk and Operations Support**

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

- **Interfacing**

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

## **TRANSITION PLAN**

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

- Coordination with Government representatives
- Review, evaluation and transition of current support services
- Transition of historic data to new contractor system
- Government-approved training and certification process
- Transfer of all necessary business and/or technical documentation
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies,

- and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
  - Applicable debriefing and personnel out-processing procedures

## EA Clause

The Offeror shall ensure that the design conforms to the DHS and CBP enterprise architecture (EA), the DHS and CBP technical reference models (TRM), and all DHS and CBP policies and guidelines as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA) such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture - Technical Framework.

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

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

All developed solutions shall be compliant with the HLS (Homeland Security) EA (Enterprise Architecture).

All IT hardware or software shall comply with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.



All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model. Submittal shall be through the CBP Data Engineering Branch and CBP EA.

In compliance with OMB mandates, all network hardware provided under the scope of this Statement of Work and associated Task Orders shall be IPv6 compatible without modification, upgrade, or replacement.

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public. All deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt.