SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12,17,23,24, & 30

1. REQUISITION NUMBER: PR20071746
PAGE 1 OF PAGES 52

2. CONTRACT NO.: HSBP1013D00006
3. AWARD/EFF. DATE: 06/03/2013
4. ORDER NUMBER:
5. SOLICITATION NUMBER: HSBP1013R0012
6. SOLICITATION ISSUE DATE:

7. FOR SOLICITATION INFORMATION CALL:
a. NAME: Robert Sieferman
b. TELEPHONE NUMBER (No collect calls): 317-614-4590
8. OFFER DUE DATE/ LOCAL TIME:

9. ISSUED BY CODE 7014
DHS - Customs & Border Protection
CBP, Procurement Directorate
Intech Two, Suite 100
6650 Telecom Drive
Indianapolis IN 46278

10. THIS ACQUISITION IS
☒ UNRESTRICTED OR ☐ SET ASIDE: 0 % FOR:
☐ SMALL BUSINESS
☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
☐ HUBZONE SMALL BUSINESS
☐ ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
☐ 8(A)
NAICS: 541612
SIZE STANDARD: $14.0 MILLION

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
☒ SEE SCHEDULE
12. DISCOUNT TERMS: Net 30
☐ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)
13b. RATING
14. METHOD OF SOLICITATION
☐ RFQ ☐ IFB ☒ RFP

15. DELIVER TO CODE
Customs and Border Protection
1300 Pennsylvania Av, NW
Washington, DC 20229
DELIVERY DATE

16. ADMINISTERED BY CODE
DHS - Customs & Border Protection
CBP, Procurement Directorate
Intech Two, Suite 100
6650 Telecom Drive
INDIANAPOLIS IN 46278

17a. CONTRACTOR/ OFFEROR CODE 940048916 FACILITY CODE
PERFORMANCE ASSESSMENT NETWORK INC
11590 N MERIDIAN ST (STE 200)
CARMEL IN 46032-5651
TELEPHONE NO.
☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER.

18a. PAYMENT WILL BE MADE BY CODE
DHS - Customs & Border Protection
National Finance Center
PO Box 68908
Indianapolis IN 46268
18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED. ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
10	Online Testing	1,000	AU		

25. ACCOUNTING AND APPROPRIATION DATA
26. TOTAL AWARD AMOUNT (For Govt Use Only): $0.00

☒ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.
☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.

☒ 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____ YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: _____

(b) (6) [redacted]

30a. SIGNATURE OF OFFEROR/CONTRACTOR (b) (6) [redacted]
President and C.E.O
30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)
30c. DATE SIGNED 5/31/13

31a. (b) (6) [redacted]
31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT) Susan Hargett-Evans
31c. DATE SIGNED 5/30/13

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 6/2011)
Prescribed by GSA - FAR (48 CFR) 53.212

CONTRACT NO.:	REQUISITION NUMBER	AWARD/EFF. DATE
HSBP1013D00006	PR20071746	06/03/2013

ADDITIONAL INFORMATION:

This is a fixed price indefinite delivery/indefinite quantity contract. Task orders shall be issued against this contract to include terms, conditions and pricing of the contract. Task orders shall be issued as requirements arise.

32a. QUANTITY IN COLUMN 21 HAS BEEN
☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED _____

32b. SIGNATURE OF AUTHORIZED GOVT. REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
		32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY (Print)	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT (Location)	
		42c. DATE REC'D (YY/MM/DD)	42d. TOTAL CONTAINERS

TABLE OF CONTENTS

Table Of Contents

SECTION I SCHEDULES 4
I.1 SCHEDULE OF SUPPLIES/SERVICES 4
I.2 ACCOUNTING and APPROPRIATION DATA 4
I.3 DELIVERY SCHEDULE 4
SECTION II CONTRACT CLAUSES 5
II.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 5
II.2 52.204-4 PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER (MAY 2011) 5
II.3 52.204-7 CENTRAL CONTRACTOR REGISTRATION (DEC 2012) 5
II.4 52.204-13 CENTRAL CONTRACTOR REGISTRATION MAINTENANCE (DEC 2012) 5
II.5 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (FEB 2012) 5
II.6 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (JAN 2013) 5
II.7 52.216-18 ORDERING (OCT 1995) 9
II.8 52.216-19 ORDER LIMITATIONS (OCT 1995) 10
II.9 52.216-22 INDEFINITE QUANTITY (OCT 1995) 10
II.10 52.222-49 SERVICE CONTRACT ACT--PLACE OF PERFORMANCE UNKNOWN (MAY 1989) 10
II.11 52.224-1 PRIVACY ACT NOTIFICATION (APR 1984) 11
II.12 52.224-2 PRIVACY ACT (APR 1984) 11
II.13 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) 11
II.14 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999) 12
II.15 52.227-14 RIGHTS IN DATA-GENERAL (DEC 2007) 12
II.16 3052.209-70 PROHIBITION ON CONTRACTS WITH CORPORATE EXPATRIATES (JUN 2006) 15
II.17 3052.215-70 KEY PERSONNEL OR FACILITIES (DEC 2003) 17
II.18 3052.242-72 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (DEC 2003) 17
II.19 3052.219-70 SMALL BUSINESS SUBCONTRACTING PLAN REPORTING (JUN 2006) 18
II.20 3052.219-71 DHS MENTOR-PROTEGE PROGRAM (JUN 2006) 18
II.21 52.232-99 PROVIDING ACCELERATED PAYMENT TO SMALL BUSINESS SUBCONTRACTORS (DEVIATION) 18
II.22 CONTRACT TYPE (OCT 2008) 19
II.23 TERM OF CONTRACT WITH OPTION(S) (MAR 2003) 19
II.24 CONTRACTING OFFICER'S AUTHORITY (MAR 2003) 19
II.25 PAYMENT AND INVOICE INSTRUCTIONS (FEB 2012) 19
II.26 ORDERING PROCEDURES - SERVICES (OCT 2007) 21
II.27 DISCLOSURE OF INFORMATION (MAR 2003) 22
II.28 SECURITY PROCEDURES (OCT 2009) 22
II.29 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011) 24
II.30 3052.204-70 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006) 25
II.31 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JUN 2006) 26

SECTION I SCHEDULES

I.1 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	Online Testing – Base Year	1.000	AU	See Attached Pricing Matrix	
20	Online Testing – Option Year 1	1.000	AU	See Attached Pricing Matrix	
30	Online Testing – Option Year 2	1.000	AU	See Attached Pricing Matrix	
40	Online Testing – Option Year 3	1.000	AU	See Attached Pricing Matrix	
50	Online Testing – Option Year 4	1.000	AU	See Attached Pricing Matrix	

Total Funded Value of Award:

I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2525USCSGLCS0927010300Z00013400HQ0116050400 130742525	
20	6100.2525USCSGLCS0927010300Z00013400HQ0116050400 130742525	
30	6100.2525USCSGLCS0927010300Z00013400HQ0116050400 130742525	
40	6100.2525USCSGLCS0927010300Z00013400HQ0116050400 130742525	
50	6100.2525USCSGLCS0927010300Z00013400HQ0116050400 130742525	

I.3 DELIVERY SCHEDULE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 1300 Pennsylvania Av, NW Washington, DC 20229	10	1.000	Established with each task order.
Customs and Border Protection 1300 Pennsylvania Av, NW Washington, DC 20229	20	1.000	Established with each task order.
Customs and Border Protection 1300 Pennsylvania Av, NW Washington, DC 20229	30	1.000	Established with each task order.
Customs and Border Protection 1300 Pennsylvania Av, NW Washington, DC 20229	40	1.000	Established with each task order.
Customs and Border Protection 1300 Pennsylvania Av, NW Washington, DC 20229	50	1.000	Established with each task order.

The estimated potential value of this IDIQ contract is $14,137,272.00 and the guaranteed minimum order on this contract is $50,000.00.

SECTION II CONTRACT CLAUSES

II.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

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

www.acquisition.gov

I. FEDERAL ACQUISITION REGULATION (48 CHAPTER 1) CLAUSES

NUMBER TITLE

II.2 52.204-4 PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER (MAY 2011)

II.3 52.204-7 CENTRAL CONTRACTOR REGISTRATION (DEC 2012)

II.4 52.204-13 CENTRAL CONTRACTOR REGISTRATION MAINTENANCE (DEC 2012)

II.5 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (FEB 2012)

II.6 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (JAN 2013)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

[] Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(2) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(3) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Pub. L. 108-77, 108-78)

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:
[Contracting Officer check as appropriate]

[X] (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (SEP 2006), with Alternate I (OCT 1995) (41 U.S.C. 253g and 10 U.S.C. 2402).

[X] (2) 52.203-13, Contractor Code of Business Ethics and Conduct (APR 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

[] (3) 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

[] (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (AUG 2012) (Pub. L. 109-282) (31 U.S.C. 6101 note).

[] (5) 52.204-11, American Recovery and Reinvestment Act—Reporting Requirements (JUL 2010) (Pub. L. 111-5).

[X] (6) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (DEC 2010) (31 U.S.C. 6101 note).

[] (7) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (FEB 2012) (41 U.S.C. 2313)

[] (8) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (MAY 2012) (section 738 of Division C of Pub. L. 112-74, section 740 of Division C of Pub. L. 111-117, section 743 of Division D of Pub. L. 111-8, and section 745 of Division D of Pub. L. 110-161).

[] (9) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (NOV 2011) (15 U.S.C. 657a).

[X] (10) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (JAN 2011) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

[] (11) [Reserved]

[] (12) (i) 52.219-6, Notice of Total Small Business Set-Aside (NOV 2011) (15 U.S.C. 644).

[] (ii) Alternate I (NOV 2011).

[] (iii) Alternate II (NOV 2011).

[] (13) (i) 52.219-7, Notice of Partial Small Business Set-Aside (JUN 2003) (15 U.S.C. 644).

[] (ii) Alternate I (OCT 1995) of 52.219-7.

[] (iii) Alternate II (MAR 2004) of 52.219-7.

[X] (14) 52.219-8, Utilization of Small Business Concerns (JAN 2011) (15 U.S.C. 637(d)(2) and (3)).

[X] (15) (i) 52.219-9, Small Business Subcontracting Plan (JAN 2011) (15 U.S.C. 637(d)(4).

[] (ii) Alternate I (OCT 2001) of 52.219-9.

[] (iii) Alternate II (OCT 2001) of 52.219-9.

[] (iv) Alternate III (JUL 2010) of 52.219-9.

[] (16) 52.219-13, Notice of Set-Aside of Orders (NOV 2011) (15 U.S.C. 644(r)).

[] (17) 52.219-14, Limitations on Subcontracting (NOV 2011) (15 U.S.C. 637(a)(14)).

[] (18) 52.219-16, Liquidated Damages--Subcontracting Plan (JAN 1999) (15 U.S.C. 637(d)(4)(F)(i)).

[] (19)(i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (OCT 2008) (10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer).

[] (ii) Alternate I (JUN 2003) of 52.219-23.

[] (20) 52.219-25, Small Disadvantaged Business Participation Program--Disadvantaged Status and Reporting (DEC 2010) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

[] (21) 52.219-26, Small Disadvantaged Business Participation Program--Incentive Subcontracting (OCT 2000) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

[] (22) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (NOV 2011) (15 U.S.C. 657f).

[X] (23) 52.219-28, Post Award Small Business Program Rerepresentation (APR 2012) (15 U.S.C. 632(a)(2)).

[] (24) 52.219-29, Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (APR 2012) (15 U.S.C. 637(m)).

[] (25) 52.219-30, Notice of Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (APR 2012) (15 U.S.C. 637(m)).

[X] (26) 52.222-3, Convict Labor (JUN 2003) (E.O. 11755).

[X] (27) 52.222-19, Child Labor--Cooperation with Authorities and Remedies (MAR 2012) (E.O. 13126).

[X] (28) 52.222-21, Prohibition of Segregated Facilities (FEB 1999).

[X] (29) 52.222-26, Equal Opportunity (MAR 2007) (E.O. 11246).

[] (30) 52.222-35, Equal Opportunity for Veterans (SEP 2010) (38 U.S.C. 4212).

[] (31) 52.222-36, Affirmative Action for Workers with Disabilities (OCT 2010) (29 U.S.C. 793).

[] (32) 52.222-37, Employment Reports on Veterans (SEP 2010) (38 U.S.C. 4212).

[X] (33) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

[X] (34) 52.222-54, Employment Eligibility Verification (JUL 2012). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

[] (35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Products Items (MAY 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[] (ii) Alternate I (MAY 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[] (36) 52.223-15, Energy Efficiency in Energy--Consuming Products (DEC 2007) (42 U.S.C. 8259b).

[] (37)(i) 52.223-16, IEEE 1689 Standard for the Environmental Assessment of Personal Computer Products (DEC 2007) (E.O. 13423).

[] (ii) Alternate I (DEC 2007) of 52.223-16.

[X] (38) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (AUG 2011).

[] (39) 52.225-1, Buy American Act--Supplies (FEB 2009) (41 U.S.C. 10a-10d).

[] (40)(i) 52.225-3, Buy American Act--Free Trade Agreements--Israeli Trade Act (NOV 2012) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

[] (ii) Alternate I (MAR 2012) of 52.225-3.

[] (iii) Alternate II (MAR 2012) of 52.225-3.

[] (iv) Alternate III (NOV 2012) of 52.225-3.

[] (41) 52.225-5, Trade Agreements (NOV 2012) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

[X] (42) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.o.s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

[] (43) 52.226-4, Notice of Disaster or Emergency Area set-Aside (NOV 2007)

[] (44) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (NOV 2007)

[] (45) 52.232-29, Terms for Financing of Purchases of Commercial Items (FEB 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

[] (46) 52.232-30, Installment Payments for Commercial Items (OCT 1995) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

[X] (47) 52.232-33, Payment by Electronic Funds Transfer--Central Contractor Registration (OCT 2003) (31 U.S.C. 3332).

[] (48) 52.232-34, Payment by Electronic Funds Transfer--Other than Central Contractor Registration (MAY 1999) (31 U.S.C. 3332).

[] (49) 52.232-36, Payment by Third Party (FEB 2010) (31 U.S.C. 3332).

[] (50) 52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).

[] (51)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

[] (ii) Alternate I (APR 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:
[Contracting Officer check as appropriate.]

[X] (1) 52.222-41, Service Contract Act of 1965 (NOV 2007) (41 U.S.C. 351, et seq).

[X] (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (MAY 1989) (29 U.S.C. 206 and 41 U.S.C. 351, et seq).

[] (3) 52.222-43, Fair Labor Standards Act and Service Contract Act--Price Adjustment (Multiple Year and Option Contracts) (SEP 2009) (29 U.S.C. 206 and 41 U.S.C. 351, et seq).

[] (4) 52.222-44, Fair Labor Standards Act and Service Contract Act--Price Adjustment (SEP 2009) (29 U.S.C. 206 and 41 U.S.C. 351, et seq).

[] (5) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (NOV 2007) (41 U.S.C. 351, et seq.).

[] (6) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (FEB 2009) (41 U.S.C. 351, et seq.).

[] (7) 52.222-17, Nondisplacement of Qualified Workers (JAN 2013) (E.O.13495).

[] (8) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAR 2009) (Pub. L. 110-247).

[] (9) 52.237-11, Accepting and Dispensing of $1 Coin (SEP 2008) (31 U.S.C. 5112(p)(1)).

(d) Comptroller General Examination of Record The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e) (1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in paragraphs (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (APR 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

(ii) 52.219-8, Utilization of Small Business Concerns (DEC 2010) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $650,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) 52.222-17, Nondisplacement of Qualified Workers (JAN 2013) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(iv) 52.222-26, Equal Opportunity (MAR 2007) (E.O. 11246).

(v) 52.222-35, Equal Opportunity for Veterans (SEP 2010) (38 U.S.C. 4212).

(vi) 52.222-36, Affirmative Action for Workers with Disabilities (OCT 2010) (29 U.S.C. 793).

(vii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(viii) 52.222-41, Service Contract Act of 1965 (NOV 2007) (41 U.S.C. 351, et seq.).

(ix) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

[] Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(x) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (NOV 2007) (41 U.S.C. 351, et seq.).

(xi) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services-Requirements (FEB 2009) (41 U.S.C. 351, et seq.).

(xii) 52.222-54, Employment Eligibility Verification (JUL 2012).

(xiii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAR 2009) (Pub. L. 110-247). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xiv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

II.7 52.216-18 ORDERING (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from 06/03/2013 through 05/31/2018

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of clause)

II.8 52.216-19 ORDER LIMITATIONS (OCT 1995)

(a) *Minimum order.* When the Government requires supplies or services covered by this contract in an amount of less than $50,000.00, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) *Maximum order.* The Contractor is not obligated to honor--

(1) Any order for a single item in excess of $2,000,000.00;

(2) Any order for a combination of items in excess of $5,000,000.00; or

(3) A series of orders from the same ordering office within 30 days that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 7 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of clause)

II.9 52.216-22 INDEFINITE QUANTITY (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after the end of the 4th option year, if exercised.

(End of clause)

II.10 52.222-49 SERVICE CONTRACT ACT--PLACE OF PERFORMANCE UNKNOWN (MAY 1989)

(a) This contract is subject to the Service Contract Act, and the place of performance was unknown when the solicitation was issued. In addition to places or areas identified in wage determinations, if any, attached to the solicitation, wage

determinations have also been requested for the following: N/A. The Contracting Officer will request wage determinations for additional places or areas of performance if asked to do so in writing no later than 7 days prior to work beginning in a specific area.

(b) Offerors who intend to perform in a place or area of performance for which a wage determination has not been attached or requested may nevertheless submit bids or proposals. However, a wage determination shall be requested and incorporated in the resultant contract retroactive to the date of contract award, and there shall be no adjustment in the contract price.

II.11 52.224-1 PRIVACY ACT NOTIFICATION (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(End of clause)

II.12 52.224-2 PRIVACY ACT (APR 1984)

(a) The Contractor agrees to--

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies--

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c) (1) Operation of a system of records, as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) Record, as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) System of records on individuals, as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(End of Clause)

II.13 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years.

(End of clause)

II.14 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

(End of clause)

II.15 52.227-14 RIGHTS IN DATA-GENERAL (DEC 2007)

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

Computer database or database means a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

Computer software-- (1) Means (i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation. Computer software documentation means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

Data means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

Form, fit, and function data means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

Limited rights means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of paragraph (g)(3) if included in this clause.

Limited rights data means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

Restricted computer software means computer software developed at private expense and that is a trade secret, is commercial or financial and confidential or privileged, or is copyrighted computer software, including minor modifications of the computer software.

Restricted rights, as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a

collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

Technical data, means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases (See 41 U.S.C. 403(8)).

Unlimited rights means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) *Allocation of rights.* (1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in--

(i) Data first produced in the performance of this contract;

(ii) Form, fit, and function data delivered under this contract;

(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and

(iv) All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause.

(2) The Contractor shall have the right to--

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;

(iii) Substantiate the use of, add, or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) *Copyright*-- (1) *Data first produced in the performance of this contract.* (i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may, without prior approval of the Contracting Officer, assert copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings, or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and an acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly by or on behalf of the Government. For computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without the prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor--

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause or, if such data are restricted computer software, the Government shall acquire a copyright license as set forth in paragraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices.* The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication, and use of data.* The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except--

(1) As prohibited by Federal law or regulation (e.g., export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless specifically authorized otherwise in writing by the Contracting Officer.

(e) *Unauthorized marking of data.* (1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g)(4) if included in this clause, and use of the notices is not authorized by this clause, or if the data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 253d, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in paragraph (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be cancelled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination will become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government will continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in paragraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of the clause from bringing a claim, in

accordance with the Disputes clause of this contract, that may arise as the result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) *Omitted or incorrect markings.* (1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized notices placed on the data at the Contractor's expense. The Contracting Officer may agree to do so if the Contractor--

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may--

(i) Permit correction of the notice at the Contractor's expense if the Contractor identifies the data and demonstrates that the correct notice is authorized; or

(ii) Correct any incorrect notices.

(g) *Protection of limited rights data and restricted computer software.* (1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall--

(i) Identify the data being withheld; and

(ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.

(3) [Reserved]

(h) *Subcontracting.* The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government those rights, the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights.* Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

(End of clause)

II.16 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]:

[_X_] 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)

II.17 3052.215-70 KEY PERSONNEL OR FACILITIES (DEC 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Contract:

PROJECT MANAGER
SOFTWARE/WEB DEVELOPER
DATABASE ARCHITECT MANAGER
TESTING CENTER DIRECTOR
SECURITY ANALYST/ENGINEER

II.18 3052.242-72 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (DEC 2003)

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the Contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COTR under the contract.

(b) The Contracting Officer cannot authorize the COTR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the Contracting Officer.

(End of Clause)

II.19 3052.219-70 SMALL BUSINESS SUBCONTRACTING PLAN REPORTING (JUN 2006)

(a) The Contractor shall enter the information for the Subcontracting Report for Individual Contracts (formally the Standard Form 294 (SF 294)) and the Summary Subcontract Report (formally the Standard Form 295 (SF-295)) into the Electronic Subcontracting Reporting System (eSRS) at http://www.esrs.gov.

The Contractor shall include this clause in all subcontracts that include the clause at (FAR) 48 CFR 52.219-9.

(End of Clause)

II.20 3052.219-71 DHS MENTOR-PROTEGE PROGRAM (JUN 2006)

(a) Large businesses are encouraged to participate in the DHS Mentor-Protege program for the purpose of providing developmental assistance to eligible small business protege entities to enhance their capabilities and increase their participation in DHS contracts.

(b) The program consists of:

(1) Mentor firms, which are large prime contractors capable of providing developmental assistance;

(2) Protege firms, which are small businesses, veteran-owned small businesses, service-disabled veteran-owned small businesses, HUBZone small businesses, small disadvantaged businesses, and women-owned small business concerns; and

(3) Mentor-Protege agreements, approved by the DHS OSDBU.

(c) Mentor participation in the program means providing business developmental assistance to aid Protege in developing the requisite expertise to effectively compete for and successfully perform DHS contracts and subcontracts.

(d) Large business prime contractors serving as mentors in the DHS Mentor-Protege program, are eligible for a post-award incentive for subcontracting plan credit. The mentor may receive credit for costs it incurs to provide assistance to a protege firm. The mentor may use this additional credit towards attaining its subcontracting plan participation goal under the same or another DHS contract. The amount of credit given to a mentor firm for these protege developmental assistance costs shall be calculated on a dollar for dollar basis and reported in the Summary Subcontract Report via the Electronic Subcontracting Reporting System (eSRS) at http://www.esrs.gov. For example, a mentor/large business prime contractor would report a $10,000 subcontract to the protege/small business subcontractor and $5,000 of developmental assistance to the protege/small business subcontractor as $15,000. The Mentor and Protege will submit a signed joint statement agreeing on the dollar value of the developmental assistance and the Summary Subcontract Report.

(e) Contractors interested in participating in the program are encouraged to contact the DHS OSDBU for more information.

(End of Clause)

II.21 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)

II.22 CONTRACT TYPE (OCT 2008)

This is a Fixed Price contract.

[End of Clause]

II.23 TERM OF CONTRACT WITH OPTION(S) (MAR 2003)

The contract term shall be for a period of one year from the date of award, subject to the Government's option to extend the term of the contract in accordance with the clause entitled, "Option to Extend the Term of the Contract" FAR 52.217-9 contained herein.

[End of Clause]

II.24 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]

II.25 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)

DHS/U.S. Customs and Border Protection
Attention: ROBERT SIEFERMAN
US CUSTOMS AND BORDER PROTECTION
6650 TELECOM DR, STE 100

INDIANAPOLIS, IN 46278

OR email: ROBERT.SIEFERMAN@DHS.GOV

(3) Contracting Officer's Representative (COR)

DHS/U.S. Customs and Border Protection
Attention: (b) (6) [redacted]
US CUSTOMS AND BORDER PROTECTION
1400 L STREET, NW
WASHINGTON, DC 20229

OR email: (b) (6) [redacted]

(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 N/A
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]

II.26 ORDERING PROCEDURES - SERVICES (OCT 2007)

Any services to be performed under this contract shall be ordered by issuance of task orders. Such task orders may be issued at any time during the period of performance of this contract provided that any task order issued shall be completed within the period specified in the order.

Ordering of services under this contract shall be accomplished by as follows:

1. The Contracting Officer (CO) will forward a task order request to the Contractor which will describe technical requirements for deliverable products, performance standards, acceptable criteria, performance schedules, etc. in sufficient detail to permit accurate estimation of cost, work, hours, etc. Where possible, requirements will be described using a Statement of Objectives and the contractor's submission will be required to employ performance-based Statements of Work, performance metrics, and quality assurance plans.

2. Within ten (10) working days after receipt of the task order request, unless a different period is specified, the Contractor will submit a written proposal responding to the Government's requirement. The contractor's proposal shall contain, as a minimum, the following:

(a) Task Requirements. A narrative description of the Contractor's understanding of the functions required to satisfy the requirements. The Contractor's proposal shall also state the purpose of the task order to ensure the Contractor's understanding of the requirement.

(b) Proposal Solution. A narrative description of the Contractor's proposed solution -- plans for performance, technical approach, and any problems envisioned.

(c) Assumptions. The proposal shall identify any assumptions on the Contractor's part used in developing the proposal and costs.

(d) Milestones and Deliverables. Definition of milestones, deliverables, and schedule for them. Include a statement of the Contractor's understanding of acceptance criteria.

(e) Work Breakdown Structure (WBS). A detailed WBS, with labor hours by skill category that will be applied to each milestone and deliverable, and the price applicable to each milestone or deliverable.

(f) Staffing Schedule. A staffing schedule by individual Contractor skill level employee.

(g) Resumes of personnel. If required. Resumes need not be provided unless personnel are proposed whose resumes have not been previously furnished to the Government.

3. After the Contracting Officer's Technical Representative (COTR) has completed an evaluation of the Contractor's proposal, the CO may conduct discussions with the Contractor to resolve any outstanding issues. Following any required discussions with the Contractor, the CO will issue a written task order incorporating the Contractor's technical and cost proposal as accepted. All task orders issued under this contract shall conform to the provisions of the contract clause FAR 52.216-18 "Ordering" and FAR 52.216-19 "Order Limitations" contained in the contract.
4. The only office(s) authorized to issue delivery orders under this contract are:

U.S. Customs & Border Protection
Office of Finance
Procurement Directorate

US CUSTOMS AND BORDER PROTECTION
OFFICE OF FINANCE
PROCUREMENT DIRECTORATE

Oral orders under this contract are not authorized.

[End of Clause]

II.27 DISCLOSURE OF INFORMATION (MAR 2003)

A. General

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract.

B. Technical Data Rights

The Contractor shall not use, disclose, reproduce, or otherwise divulge or transfuse to any persons any technical information or data licensed for use by the Government that bears any type of restrictive or proprietary legend except as may be necessary in the performance of the contract. Refer to the Rights in Data clause for additional information.

C. Privacy Act

In performance of this contract the Contractor assumes the responsibility for protection of the confidentiality of all Government records and/or protected data provided for performance under the contract and shall ensure that (a) all work performed by any subcontractor is subject to the disclosure restrictions set forth above and (b) all subcontract work be performed under the supervision of the Contractor or their employees.

[End of Clause]

II.28 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]

II.29 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]

II.30 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 60 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.

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)

II.31 3052.204-71 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.

(End of Clause)

CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

Attachment 1 – Statement of Work

Attachment 2 – Contract Pricing Matrix

ATTACHMENT 1 – STATEMENT OF WORK

Statement of Work (SOW)
Procurement Directorate
Office of Human Resources Management

1. **BACKGROUND:**

U.S. Customs and Border Protection (CBP) requires services for the automated assessment of candidates' knowledge, skills, abilities, and competencies for law enforcement positions. CBP is responsible for developing, implementing, and analyzing assessments for selection, career development, and promotion into mission-critical occupations within the Department of Homeland Security (DHS). These positions are in U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement (ICE), and Customs and Immigration Services (CIS). The automated assessment services are used to support promotions within these agencies.

CBP Automated Testing Service (CATS) consists of different types of assessments across many types of programs. Currently there are seven assessment programs. The three largest programs are the promotional testing programs for Border Patrol Agent, CBP Officer/Agriculture Specialist, and Special Agent. There will be up to eleven assessment programs during the period of performance. Within each program, assessments are grouped in batteries. There are two to four assessments per battery, depending on the program. The assessments for a program are unique to that program. These assessments will be updated at various times during the performance period. See Diagram 1 below for the content of each battery by program.

Diagram 1 CATS Assessment Batteries by Program

	Program	Assessment Type					
		Job Knowledge	*Logical Reasoning*	*Job Simulation*	*Writing*	*Writing Sample*	*Biodata*
1	*Border Patrol Agent (BPA)*	X	X	X	X		
2	*CBP Officer/ Agriculture Specialist (CBPO/AS)*		X	X	X		
3	*Special Agent (SA14)*	X	X	X	X		
4	*Criminal Investigator (CI)*		X		X	X	X
5	*Management Program Analyst (MPA)*		X	X	X		
6	*Intelligence Analyst (IA)*		X		X		
7	*Immigration Enforcement Agent (IEA)*		X				X
8	*New Program 1*		X	X	X		
9	*New Program 2*		X		X		
10	*New Program 3*		X				X
11	*New Program 4*		X	X	X		

*Note = "X" denotes required assessment. Program names may vary.

Typically each program tests for a 2-3 week period each year, except BPA which currently has two testing periods per year. However, some programs may decide to offer more than one testing period annually. Programs typically do not test simultaneously but scheduling for multiple programs can occur during the same period.

For each program's scheduling and testing period, a list of candidates with associated e-mail addresses is provided to the Contractor by CBP. The Contractor distributes e-mail scheduling notifications to the candidates, who in turn access the Contractor's automated scheduling system to self-select the appropriate assessments and schedule their testing appointment date, time, and location. Using the automated scheduling service, candidates can schedule test appointments at designated locations in the U.S. and internationally. These test locations are provided by the Contractor and are proctored. CBP develops the assessments and provides them to the Contractor to automate and administer. The Contractor provides the raw assessment data to CBP for scoring. CBP translates raw assessment data into scores for each candidate and provides those scores to the Contractor. The Contractor makes the scores available to each

candidate through each candidate's online account. Candidates can access their scores at any time and candidates who completed the test outside of this online process also access their scores through the Contractor's system.

2. **KEY DEFINITIONS:**

- Static site: A facility that is a permanent automated testing center.
- Mobile site: A facility that is a temporary automated testing center.
- International site: A facility that is located outside of the United States or U.S. territories.
- Candidate: An individual who either has a historical score on an assessment or is interested in taking an assessment battery offered by CBP's CATS.
- Assessment: A specific test. May be traditional multiple-choice, job simulation multiple-choice, or narrative. Assessments are defined by name and series number and are unique to each occupation.
- Battery: A selection of assessment types and series numbers (to be determined by program and year) that are combined to be delivered to a candidate during a scheduled test session.
- CO: Contracting Officer
- COR: Contracting Officer's Representative

3. **SCOPE:**

The Contractor shall provide these broad functions:

(a) a system that shall automate and maintain assessment batteries in accordance with CBP requirements,
(b) the upload of historical candidate information, testing history, and test results into a candidate registration and scheduling system,
(c) an automated registration and self-scheduling service for candidates using secure individual online accounts, including the capability to send system generated e-mail notifications to candidates,
(d) proctored computer based administration of assessments and candidate exit survey to include providing testing facilities, proctors, and all testing equipment,
(e) the transfer of raw assessment data and survey results to CBP,
(f) loading scored assessment data received from CBP into the system for each candidate,
(g) communication of candidate results, to include sending email notification of results availability to candidates, the ability for candidates to access their online account to view results at any time, the ability for candidates to download from their online accounts a feedback guide provided by CBP, and
(h) performance in accordance with CBP web services requirements (see Task 5.0. Web Service Requirements).

4. **TASKS:**

4.1 Task 1. Automate assessments.

4.1.1 The Contractor shall convert CBP provided assessments from Microsoft Word documents into computer based assessments. See Appendix 1, Projected Workload for additional information on assessments to be automated. Refer to Attachment 1 for sample test items. The assessments shall be grouped into batteries as shown in Table 1. The BPA, CBPO/AS, and SA14 programs shall each have two assessment batteries. The COR shall designate which battery the Contractor shall use. Generally, one battery is used at a time. The alternate is used on a case-by-case basis upon approval of the COR. The Contractor's testing system shall meet the following requirements:

a. Present instruction screens and a practice test to learn system navigation prior to the beginning of the assessment.
b. Require candidates to acknowledge a confidentiality agreement prior to beginning the assessment.
c. Display one test question per screen.
d. Display question number and total number of questions.
e. Allow candidates to navigate back to the previous question.
f. Allow candidates to mark questions for later review.
g. Present candidates with a view of questions marked for review and any unanswered questions and allow candidates to easily navigate to these questions or answer them from this screen.
h. Provide a single screen review of questions and answers at the end of the test and allow candidates to change responses prior to final submission of the test.
i. Automate enforcement of per assessment time limits and total assessment session time limits. The system shall allow these time limits to be extended to provide a reasonable accommodation on a per candidate basis

when approved by the COR. Total assessment session duration varies depending on assessments selected for inclusion. Appendix 1 Tables 4 and 5 indicate the session durations that can occur and their expected frequency for domestic and international testing, respectively.

j. Display countdown clock and progress bar that shall be visible throughout the test.
k. Present assessments in a fixed order within each program.
l. Allow supplemental test materials (e.g., simulated emails, memos, documents) to be presented to the candidate.
m. Present candidates with an exit survey, to be approved or provided by CBP, upon conclusion of each assessment battery.
n. Provide for a Failure Recovery protocol in case of emergency stoppages of the assessment session, power failures, and computer failure.
o. Capture test data including but not limited to responses, item latencies, assessment start time, and assessment end time.
p. Require user authentication.
q. Display branding that is individualized to each program. Branding shall be approved by the COR.

4.1.2 The Contractor will provide CBP the opportunity to review and conduct acceptance testing of the assessment automation after initial production, when changes are made, and prior to each testing period.

4.1.3 The Contractor shall immediately correct any errors identified in system functioning at no cost to CBP.

4.1.4 The Contractor shall ensure that the test administration system is stable and reliable. In the event it is necessary to retest a candidate due to system failure, the Contractor shall retest the candidate at no cost to CBP.

4.2 Task 2. Maintain assessments.

4.2.1 The Contractor shall make minor edits to the automated systems, as requested by the COR, at no additional cost to CBP. Minor edits include, but are not limited to, name changes due to government reorganizations, typos missed in the review process, etc. These edits shall be completed within 5 business days of the submission of the request. Any errors found in the production version of the automated assessments will be corrected immediately.

4.2.3 The Contractor will replace existing assessments within batteries with new versions when provided by the COR.

4.3 Task 3. Provide automated candidate registration and self-scheduling service.

4.3.1 The Contractor shall provide a web-based automated registration, scheduling, and score reporting service. This service shall meet but is not limited to the following requirements:

a. Use candidate information provided by the COR to create and maintain a secure user account for each candidate. The COR will provide the Contractor an ascii file with candidate information including but not limited to unique identifier, email address, and historical assessment results. See Attachment 2 for a sample of this data file content.
b. Provide candidates the capability to schedule during the program's scheduling period and reschedule test sessions. The COR shall provide the Contractor the dates of the scheduling periods for each program. The system shall allow candidates to view test session appointment information, including date, time, and address.
c. Allow candidates to select assessments to be taken within a test battery in accordance with the business rules described in 3.2 and 3.3.
d. The Contractor's system shall allow candidates to request reasonable accommodation in accordance with the American's with Disabilities Act. The system shall allow candidates to cancel a request for an accommodation. Accommodations must be approved by the COR. The system shall automate notification of CBP and provide CBP with the ability to approve or disapprove an accommodation.
e. Upon approval of the COR, candidates shall be allowed to schedule and complete assessments outside of the pre-determined scheduling and testing periods. These determinations are made on a case-by-case basis.
f. The Contractor shall document assessments scheduled outside of the usual testing period and provide reports to the COR (see section 5. Deliverables and Delivery Schedule).

g. Provide candidates the capability to view their scores in an online feedback report which shows current scores for all assessments completed by that candidate. Additionally, the two most recent feedback reports prior to the current report must be available to each candidate, as applicable. Candidate access to feedback reports shall be capable of being turned on or off as requested by the COR.

4.3.2 The Contractor shall ensure that the following business rules are programmed into the Contractor's scheduling system.

a. BPA and CBPO/AS Eligibility for Assessment: A candidate's eligibility to complete an assessment shall be determined by the candidate's Grade Level and previous test date. Both the candidate's current Grade Level and last test date for each test shall be included in the data sent to the Contractor from the COR and shall be stored with the candidate's record in the Contractor's database.
b. BPA Candidate Grade Level Eligibility: If the candidate's Grade Level is GS-11 or GS-12, results for the Job Knowledge, Writing, and Logical Reasoning tests shall all be required; the Job Simulation Exercise shall be optional for those candidates. If the candidate's Grade Level is GS-13 or greater, results for the Writing and Logical Reasoning tests, and Job Simulation Exercise shall be required; the Job Knowledge test shall not be available for these candidates.
c. CBPO/AS Candidate Grade Level Eligibility: If the candidate's Grade Level is GS-11 or GS-12, results for the Writing and Logical Reasoning tests shall be required; the Job Simulation Exercise shall be optional. If the candidate's Grade Level is GS-13 or greater, results for the Writing and Logical Reasoning tests, and Job Simulation Exercise shall be required.
d. SA14 Eligibility for Assessment: If a candidate has never taken one of the assessments, then all of the assessments are MANDATORY.

   SA14 Candidate Grade Level Eligibility: There is not a grade level eligibility business rule for SA-14 Special Agents.
e. Candidate Retest Eligibility: If the candidate has a score for any assessment listed in the candidate's account, the candidate is not required to retake that assessment. The candidate may choose to retake an assessment provided that one year after the last assessment date minus 28 days is not later than the last day the assessments are being offered in the new testing cycle.

4.3.3 The scheduling system shall display to the candidate the assessment status for each assessment based on the above business rules. Assessment status shall be defined as follows:

a. Eligible: The candidate has previously taken the assessment and a year after the last assessment date minus 28 days is not later than the last day the assessments are being offered in the new testing cycle.
b. Ineligible: The candidate has previously taken the assessment and a year after the last assessment date minus 28 days is not later than the last day the assessments are being offered in the new testing cycle. The candidate may NOT retake the assessment.
c. Mandatory: The candidate has never taken the assessment and must take the assessment based on the job requirements.
d. Optional: The candidate has never taken the assessment and may choose to either take the assessment or not take the assessment based on the job requirements.

4.3.4 The Contractor's scheduling system shall allow candidates to select their test location in accordance with the following:

a. The COR shall provide the Contractor a candidate file that shall include candidate work zip codes. The Contractor's system shall identify static test sites located within 120 miles driving distance of the candidate's work zip code in the United States and U.S. territories.
b. If a static site is not available within 120 miles of the work zip code, a mobile site shall be provided by the Contractor within 120 miles of the work zip code. The location of this mobile site shall be approved by the COR.
c. The system shall allow candidates to enter an alternate zip code which will be used for identifying test sites within 120 miles.
d. The Contractor shall be able to provide test centers in the U.S., including U.S. Virgin Islands, Puerto Rico, Guam, Saipan, and international locations, including Europe, Asia, Canada, Mexico, and Central America.
e. The Government shall provide the Contractor with historical data (i.e. zip codes) that show where test centers have been required in the past. (See Attachments 3a and 3b for zip codes)

f. The Contractor shall have the capability to add secure static and/or mobile testing sites upon request of the COR within three days of request.

4.3.5 The scheduling system shall allow the candidate to select the session date and time from among all available sessions during the testing period at the selected location. Sessions must be available on multiple days and times within the testing period. The Contractor shall provide weekend or evening sessions as required.

4.3.6 The Contractor's system shall generate and send e-mail notifications to candidates for test-related events, including but not limited to, scheduling, confirmation and score report notifications.

a. Email content shall be specific to each program and testing or scheduling period and shall be approved by the COR prior to each scheduling and testing period.
b. The Contractor shall incorporate revisions to the notifications provided by the COR as needed. Requested changes shall be completed with 5 business days of the request.

4.3.7 The Contractor shall provide 24/7 technical support to manage any problem candidates may have regarding the ability to create and/or access candidate accounts for selecting assessments, scheduling, rescheduling and canceling appointments, and viewing score reports.

4.3.8 The Contractor's system shall provide CBP access including but not limited to the following information and capability:

a. Access to candidate information, including but not limited to candidate scheduling status, testing status, location of testing site, assessment scores, system generated communications including date and time stamp, and accommodation request, within each testing program.
b. Access to all current and historical testing.
c. Ability to add candidates, assign test batteries to candidates, schedule candidates, track candidates, and communicate with candidates via automated configurable emails, including resending system generated emails.
d. Provide a listing of candidates by program, by test battery, and by scheduling and testing status.
e. Identify candidates who request to test in an international location, including the international city name, zip code, and country, by testing period and by program.
f. Identify candidates who request ADA accommodations. Access to the status of the request, the ability to make and read comments and scheduling needs shall be provided, and the ability to enter adjudications shall be provided.

4.4 Task 4. Administer proctored assessments.

4.4.1 The Contractor shall administer the assessment batteries at static and mobile test administration facilities. Static sites shall be provided within 120 miles of the following cities:
Mobile, AL; Phoenix, AZ; Tucson, AZ; Yuma, AZ; Los Angeles, CA; San Diego, CA; San Francisco, CA; Denver, CO; Miami, FL; Orlando, FL; Atlanta, GA; Savannah, GA; Chicago, IL; Indianapolis, IN; New Orleans, LA; Boston, MA; Baltimore, MD; Bangor, ME; Fairfield, ME/Waterville, ME; Houlton, ME; Detroit, MI; Minneapolis, MN; Minot, ND; Williston, ND; Newark, NJ; Las Cruces, NM; Albuquerque, NM; Las Vegas, NV; Buffalo, NY; New York, NY (or preferably Long Island near JFK); Potsdam, NY/Canton, NY; St. Louis, MO; Tampa, FL; Thief River Falls, MN/Grand Forks, ND; Charlotte, NC; Tulsa, OK; Philadelphia, PA; Charleston, SC; Memphis, TN; Corpus Christi, TX; Dallas, TX; Del Rio, TX; Edinburg, TX/(McAllen, TX); El Paso, TX; Houston, TX; Laredo, TX; San Antonio, TX; Salt Lake City, UT; Burlington, VT/Williston, VT; Bellingham, WA; Seattle, WA; Spokane, WA; Washington, DC.

If a static site is not available within 120 miles of these locations, the Contractor shall provide a mobile site at no additional cost to CBP.

4.4.2 The Contractor shall ensure the test administration facilities, whether static or mobile, are secure, distraction free, quiet testing environments, and shall otherwise meet acceptable standards for a commercial marketplace computer-based testing environment. The test administration facilities shall have pens, scratch paper, and highlighters available for candidate use. The test administration facilities shall have a functioning printer.

4.4.3 The Contractor shall complete all testing within the program testing period, unless testing outside of the testing period is approved by the COR.

4.4.4 At each test administration facility, the Contractor shall provide a proctor to monitor the testing and follow documented testing protocols. Test proctors at contracted locations shall wear name badges or shall otherwise self-identify themselves as contractors in support of CBP in any in-person interaction or correspondence. The test proctor shall be:

a. trained by the Contractor in the administration of tests, test security standards, and technology troubleshooting,
b. proficient in English,
c. trained in the administration of the Contractor's testing system, and
d. able and available to:
    1. greet candidates as they arrive,
    2. check-in and check-out candidates,
    3. verify candidate identity prior to the assessment,
    4. print test related materials and provide this material to candidates,
    5. monitor candidates throughout the test sessions,
    6. be qualified to provide candidates with assistance throughout their testing appointments, such as, but not limited to, resolving environmental problems, troubleshooting system problems, rescheduling candidates when the test center is unable to accommodate a completed test appointment, etc., and
    7. securely dispose of assessment related materials.

4.4.5 The Contractor shall properly identify and ensure the correct identity of the on-site candidates. At each testing site, the Contractor shall:

a. provide CBP with a daily verified roster and record of attending/non-attending candidates,
b. have a secure encryption procedure to transmit and receive roster information, and
c. have the capability to transmit attendance information and provide incident reports.

4.4.6 Upon approval by the COR, the Contractor shall make appropriate accommodations for Americans with Disabilities Act (ADA) related disabilities in accordance with the Section 508 Guidelines. These sessions represent approximately 1 of 1,000 candidates. CBP shall provide directions for conducting the assessment to meet ADA accommodation guidelines.

4.5 Task 5. Ensure adherence to test administration protocol.

4.5.1. The Contractor shall provide the COR with a proctor's manual documenting the administration protocol, including a supplement to the proctor's manual that addresses ADA accommodations. See Section 5.0 for Deliverable Schedule. The administration protocol shall address emergency evacuations of the site during the testing session, power failures and computer failures, address ADA related accommodations as outlined by CBP, and matters related to candidates who are suspected of cheating. The administration protocol shall include procedures for reporting any incident or unusual occurrence during a test session. The administration protocol shall provide a way for the assessment administrator to securely access assessment materials that are unique to each candidate and send candidate information to the Contractor and securely dispose of any paper generated test material.

4.5.2 The Contractor shall provide the COR a plan for how the Contractor shall ensure the test administration protocol is followed. This plan should also address what will occur if a proctor is not present or is late to a testing session. In the event it is necessary to retest a candidate due to failure to follow test administration procedures, the Contractor shall retest the candidate at no cost to CBP.

4.6 Task 6. Report assessment results.

4.6.1 Upon request of the COR, the Contractor shall provide the raw assessment data to CBP for scoring. The data shall be provided in the format shown in Attachment 2, "Data File Layout." In the section that shows format that the vendor sends to CBP. CBP will provide the score results to the Contractor in ascii format as shown in Attachment 2, "Data File Layout." In the section that shows format that is provided to the vendor by CBP.

4.6.2 The Contractor shall, upon receipt of scored results, update candidate records with the assessment scores and display the scores in an automated score report, approved by the COR. This score report shall show the most current

scores for each assessment taken by the candidate. The system shall allow candidates to view, print, and download the score report.

4.6.3 The Contractor's system shall allow candidates to view, print, and download a feedback guide (pdf), to be provided by the COR. Each program will have a unique feedback guide, which provides an explanation to candidates of how scores were calculated and how to interpret their score report and their two prior score reports.

4.6.4 The Contractor shall notify candidates via email when score results are made available.

4.7 Task 7. The Contractor shall document activities and provide reports to CBP as identified in Section 5 Deliverables and Delivery Schedule (Diagram 2). Report definitions are listed below.

a. Scheduling Report: A daily cumulative report which summarizes scheduling activity for a specific program during the specified scheduling time frame.
b. Testing Report: A daily cumulative report which summarizes testing activity for a specific program during the specified testing time frame.
c. Ad hoc Incident Report: An ad hoc report which provides information on any incident that has been reported by a proctor during the contract period of performance.
d. International Testing Report: A report of all candidates who indicated, during a program's scheduling period, the need for international testing.
e. Ad hoc Retest Activity Report: An ad hoc report which provides information on retest activity for each testing program during the contract period of performance.
f. Ad hoc Americans with Disability Act (ADA) Report: An ad hoc report which provides information on candidates who have requested an ADA accommodation.
g. Ad hoc Late Tester Report: An ad hoc report which provides information on candidates who have been approved by the COR to take an assessment battery outside of the specified testing period for a program.
h. End of month detailed report supporting invoice: A detailed report of testing activity to support the invoice.

4.8 Task 8. Web service requirements.

4.8.1 The Contractor must complete all electronic data transfers using web services. This requirement applies to both data provided to CBP as well as data provided from CBP.

4.8.2 Technical Requirements of Web Services. All Contractor supplied data must be made available via secure web services. This data shall be accessible via web services that return data in an agreed upon XML format. The web service shall also accept, as parameters, filter criteria such as an effective date. The Contractor's web service must conform to the following technical requirements:

a. The web service must be WS-I Basic Profile 1.1 compliant;
b. The web service must be secured via TLS and AES-256 bit encryption;
c. The web service must provide an authentication mechanism that ensures only authorized requests are processed;
d. The web service must process requests under one second;
e. The web service shall execute against and return current, up-to-date data;
f. The web service shall be available for use at all times, twenty-four (24) hours per day, seven (7) days per week;
g. The Contractor shall provide a description of their web service using a standard WSDL document;
h. The Contractor shall provide an XML schema to describe the result set returned by the web service;
i. The Contractor shall provide detailed explanation for any error condition that may be raised as a result of web service operation. The Contractor shall provide this information in the form of a list containing all possible error codes and their description.
j. The Contractor shall provide end user documentation for their web service.

4.8.3 The following expectations shall be adhered to by the Contractor during the contract term:

a. In performing the work, the Contractor shall adhere to commercial marketplace requirements that define:
    1. Web Service method signatures;
    2. Input Parameters (filter criteria);
    3. Output fields;

4. XML Schema of the result set returned by web service; and
5. Any additional business rules.

b. CBP shall be given the opportunity for acceptance testing of the Contractor provided web service.
c. The Contractor shall notify the COR no less than ninety (90) days of any modifications made to the web service that shall require modifications to CBP consuming applications.
d. All production versions of the deployed web service shall be available in production and removed only upon request from the CO or with CBP's explicit permission.
e. The Contractor shall notify the COR at least twenty-four (24) hours in advance of any web service maintenance that shall require web service down time.
f. The Contractor's web service support shall have a response time to CBP of twenty-four (24) hours or less; however, the Contractor's web service support does not need to be available twenty-four (24) hours per day, seven (7) days per week.
g. Authorization from CBP is required before sending any miscellaneous documentation that needs to be submitted to CBP outside of a web service interface (i.e. via email). Safeguards must also be put in place to protect the Personally Identifiable Information (PII) by encrypting documents prior to sending to CBP via email.

5. DELIVERABLES AND DELIVERY SCHEDULE:

The Contractor is required to submit numerous reports and deliverables to the COR throughout the contract performance period, as defined below.

Diagram 1 Deliverables and Delivery Schedule

	Deliverable	Description	Delivery/ Frequency	Submit To
1	Historical data upload	Historical data provided by CBP shall be loaded into the scheduling system	on or before 10 weeks after contract award	
2	Scheduling system UAT	Initial user testing shall be available	on or before 10 weeks after contract award	
3	Proctor manual	Manual documenting the administration protocol, including a supplement to the proctor's manual that addresses ADA accommodations as described in Task 5	On or before 3 months after contract award	COR
4	Scheduling system production	Full functionality of the scheduling system shall be available	on or before 4 months after contract award	
5	Initial UAT of first assessment program	User review of assessments for first assessment program in UAT environment	on or before 4 months after contract award	
6	Second UAT of first assessment program	User review of changes Contractor made based on initial UAT	on or before 5 months after contract award	
7	Final UAT of first assessment program	Review of operational assessment in production environment	on or before 6 months after contract award	
8	First assessment program operational	Capable of delivering candidate testing for the first assessment program	Within two weeks of completion of final UAT	
9	Initial UAT of second assessment program	User review of assessments for second assessment program in UAT environment	on or before 5 months after contract award	
10	Second UAT of second assessment program	User review of changes Contractor made based on initial UAT	on or before 6 months after contract award	

11	Final UAT of second assessment program	Review of operational assessment in production environment	on or before 7 months after contract award	
12	Second assessment program operational	Capable of delivering candidate testing for the first assessment program	Within two weeks of completion of final UAT	
13	Initial UAT of third assessment program	User review of assessments for third assessment program in UAT environment	on or before 6 months after contract award	
14	Second UAT of third assessment program	User review of changes Contractor made based on initial UAT	on or before 7 months after contract award	
15	Final UAT of third assessment program	Review of operational assessment in production environment	on or before 8 months after contract award	
16	Third assessment program operational	Capable of delivering candidate testing for the first assessment program	Within two weeks of completion of final UAT	
17	Daily Cumulative Scheduling Report	Each program has its own set of scheduling periods throughout the year. Each scheduling period typically lasts 2-3 weeks. During each scheduling period, the Contractor shall submit a daily cumulative report. The Report shall include: the number and percent of total candidates who have selected their assessments, the number and percent of candidates who have schedule an assessment appointment, and the number and percent of total candidates who have not found an available appointment time, date, or test center location and have therefore requested assistance with the scheduling process.	Daily, during each scheduling period	COR
18	Exit Survey Data Report	The Contractor shall provide raw data and a summary report of the exit survey. The raw data report shall include the name of the assessment battery, the location of the test administration facility, assessment date, and responses to all survey items and response options. The Contractor shall provide a summary report of the exit survey data will shall include but not be limited to candidate response frequencies for all question options.	Within three business days of conclusion of testing	COR
19	Test Response Report	The Contractor shall provide raw data of candidate responses, as indicated in attachment 2.	Within five business days of conclusion of testing period	
20	Daily Cumulative Testing Report	Each program has its own set of testing periods throughout the	Daily, during each testing	COR

		year. Each testing period typically lasts 2-4 weeks. During each testing period, the Contractor shall submit a daily cumulative report. The Report shall include: the number and percent of total candidates who have completed the assessment appointment, the number and percent of total candidates who checked-in to their scheduled appointment but did not complete (i.e., incomplete) their appointment, the number and percent of total candidates who failed to show up for their assessment appointment (i.e., no shows).	period	
21	Ad hoc Incident Report	The Contractor shall ensure that CBP shall have the capability to make online ad hoc inquiries to the CATS database to obtain information on any incident that has been reported by a proctor during the contract period of performance. The Ad hoc report shall provide the following: candidate name, candidate ID, date, time, test center location, proctor name, test program name, description of incident, description of the Contractor's corrective action, and status of the incident (e.g., ongoing investigation, closed).	As determined by COR	COR
22	International Testing Report	The Contractor shall provide a report, by testing program, of candidates who shall require international testing accommodations. The report shall include the following information: candidate name, candidate ID, international zip code, city, and country.	The day after the conclusion of each scheduling period	COR
23	Ad hoc Retest Activity Report	The Contractor shall ensure that CBP shall have the capability to make online ad hoc inquiries to the CATS database to obtain information on retest activity for each testing program during the contract period of performance. The Ad hoc report shall allow CBP to specify the parameters of the report, including the date range and assessment name, to obtain a summary of retest activity.	As determined by the COR	COR
24	Ad hoc Americans with Disability Act (ADA) Report	The Contractor shall ensure that CBP shall have the capability to make online ad hoc inquiries to the CATS database to obtain information on candidates who	As determined by the COR	COR

		have requested an ADA accommodation during the contract period of performance. The report shall allow CBP to specify the parameters of the report, including the date range and/or testing program, and shall include the following information: candidate name, candidate ID, request date, ADA request, request status (i.e., pending, complete, and denied), accommodation type, and note.		
25	Ad hoc Late Tester Report	The Contractor shall ensure that CBP shall have the capability to make online ad hoc inquiries to the CATS database to obtain information on candidates who have been approved by the COR to take an assessment battery outside of the specified testing period for a program. The report shall include the following information: candidate name, candidate ID, testing program, reason for late testing request, request status (pending CBP approval, CBP approved, CBP denied), status of scheduling (pending, scheduled, cancelled), status of testing appointment (pending, completed, cancelled, or no show), and notes. CBP shall require e-mail notifications to one or more CBP e-mail address, to be specified by the COR, when activity around a request status, status of scheduling, and status of testing are generated.	As determined by the COR	COR
26	End of month detailed report supporting invoice	The Contractor shall submit a detailed report of the previous months testing activity at the beginning of each month, as a supplement to the invoice. The report shall include all testing activity within the calendar month. The report shall include the following information: candidate last name, candidate first name, login ID, program, test center name, appointment date, appointment time, mobile indicator, status (i.e., complete, incomplete, no show), appointment length in minutes, and cost.	Each month with Contractor's invoice	COR
27	Quality Control Plan (QCP).	The Contractor shall establish and implement a complete Quality Control Plan (QCP) to assure the requirements of the Contract are	With Contractor's proposal	CO

		met. The QCP is a system for identifying and correcting deficiencies in the quality of services before the level of performance becomes unacceptable. The QCP shall be prepared by the Contractor and provided to the CO and COR as part of the proposal for review and acceptance by the Government. The QCP is a living document and may be subject to change depending on the needs of the contract. When the QCP is revised, the Contractor is required to provide an updated QCP to the CO and COR for acceptance.		
28	Web Service	The Contractor shall submit its proposed web service to the Government for acceptance.	With Contractor's proposal	CO
29	Transition Plan	The Contractor shall provide a transition-in and transition-out plan. The plan shall support CATS within the purview of providing any required transition planning or program execution associated with meeting the agreed to transition in and out timeline, as directed by COR. This includes the following types of tasking: • Coordination with Government representatives • Review, evaluation and transition of current services • Transition of historic data • Transfer of all necessary business and/or technical documentation Transfer of Government Furnished Information (GFI)	With Contractor's proposal	CO
30	Security Authorization	The Contractor must conduct and complete all required procedures and documentation resulting in a successful Security Authorization of their system or systems by the Department of Homeland Security (DHS) and/or US Customs and Border Protection (CBP), whether hosted internally within DHS or CBP networks or hosted externally.	After contract award	COR
31	CATS Security Plan	Security Scan Results for CATS Servers (using Nessus and AppDective from Contractor) including:	After Contract award	COR

		• System Boundary Diagram • System Hardware Inventory List • System Software Inventory List Contractor Contingency Plan		

6. **GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION:**

The Government shall furnish the Contractor, for use in direct performance of this contract, the necessary assessments, test related materials, and candidate information including historical assessment results. See Appendix 1 for a list of the Government –Furnished assessments provided throughout the performance period.

7. **PLACE OF PERFORMANCE:**

All work shall be performed at the Contractor's site and vendor testing centers.
No testing is to be performed on Government observed holidays. However, the Contractor's system (i.e., CATS) shall be operational 365 days a year.

8. **QUALIFICATIONS OF KEY PERSONNEL:**

8-1. The Project Manager shall have at least 5 years experience in managing all aspects of an automated testing service project, including: defining, scoping, and managing project requirements; managing and executing all steps within a project's lifecycle; communicating internally and externally about the project; testing, validating, and implementing programs; and daily reporting.

8-2. The Software/Web Developer shall have at least 3 years experience in preparing the interactive screen dialogues and screen questions and shall have demonstrated trustworthiness in observing the necessary security in handling confidential assessment materials.

8-3. The Database Architect Manager shall have at least 5 years experience in manipulating and storing sensitive data using the most secure methods available, and shall have experience leading teams through the integration and development process.

8-4. The Testing Center Director shall have at least 3 years experience in managing nationwide and international testing programs, including: procuring testing sites, scheduling, training of test administrators, overseeing test administrations, and leading ongoing audits of sites, equipment, and personnel.

8-5. The Security Analyst/Engineer shall have at least 5 years' experience and knowledge in IT security and should hold at least an IAT/IAM Level II certification, or at the minimum a IAT/IAM Level I (see DoD Directive 8570.1 for additional information). This shall include: (a) experience – prior or current experience in providing security-related services to government agencies and departments or other organizations completing numerous successful security authorization processes that reflect the structure and discipline of successful security practices and methodologies; and (b) knowledge – which can be demonstrated through acquiring of general information system security related academic degrees, or professional certification or specialized product certification programs.

9. **SECURITY:**

The requirements of security ensure that the process of establishing and maintaining a framework and supporting management structure and processes provide assurance that information security strategies are aligned with and support the business objectives of CBP and DHS, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

CBP Program Offices shall provide personnel (System Owner and Information System Security Officers) with the appropriate clearance levels to support the Security Authorization (SA), (formerly Certification & Accreditation (C&A)) processes under this Agreement in accordance with the current version of the DHS MD 4300A *Sensitive Systems Policy* and *Sensitive Systems Policy Handbook*, CBP HB-1400-05D, *Information Systems Security Policies and Procedures Handbook*, 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 SA process. In addition, all SAs will be performed using the DHS SA 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.

9.1. General Security

a. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. Contractor shall conform to all security policies contained in the *U.S. Customs and Border Protection Information Systems Security Policies and Procedures Handbook*, CIS HB 1400-05D.

b. 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*."

9.1.1. Security Clearances: Personnel Security Background Data

Performance under this SOW is considered sensitive but unclassified and a security clearance is not required.

a. All personnel employed by the Contractor for work performed under this Statement of Work (including any new personnel hired as replacement(s) during the term of this contract) must receive a favorable suitability determination for employment by the Office of Internal Affairs-Personnel Security Division (PSD) following completion of a CBP background investigation. Periodic reinvestigations will be required pursuant to applicable CBP requirements (currently 5 years). Federal investigations completed by other federal entities may be given reciprocal consideration in accordance with CBP policy. A preliminary (a.k.a. provisional) determination may be rendered by PSD thereby authorizing the individual to begin work prior to completion and final adjudication of the investigation (access to systems may be restricted until completion and final adjudication of the investigation. Any individual employed under this contract who is determined unsuitable by PSD will be removed from all work on CBP contracts immediately.

b. All contract personnel should orient themselves with the CBP Security Policy and Procedures Handbook (HB1400-02B), August 13, 2009, Volume IV, Chapter 13, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.

   The majority of data processed on Customs and Border Protection (CBP) systems is considered Sensitive But Unclassified (SBU), For Official Use Only (FOUO). The network used to transport this data is the Department of Homeland Security (DHS) OneNet.

c. The Contractor shall submit within ten (10) working days after award of the this contract a list containing the full name, social security number, and date of birth of those employees who claim to have already successfully passed a background investigation by CBP, or submit such information and documentation as may be required by the Government to have a background investigation performed. The background information must be correct and reviewed by the designated CBP Security Official for completeness. Normally, information requested for a background investigation consists of:

   - An SF-85P, "*Questionnaire for Public Trust Positions*"
   - An SF-86, "*Questionnaire for Sensitive Positions (For National Security*"
   - TDF 67-32.5, "*U.S. USCS Authorization for Release of Information*"
   - An FD-258, "*Fingerprint Chart*"
   - A Financial Statement

   Failure of any Contractor personnel to successfully pass a background investigation shall be cause for the candidate's dismissal from the project. The Contractor shall immediately recommend an equally qualified replacement with similar or equal experience. The recommended replacement shall be approved by the Contracting Officer and the COR. This policy also applies to any personnel hired as replacements during the term of the contract.

d. The Contractor shall immediately notify the Contracting Officer (CO) and the Contracting Officer Technical Representative (COR) of any personnel changes. Written approval for confirmation purposes is also required if there has been a telephone notification. This includes resignations, terminations, and reassignment.

e. The Contractor shall also notify the CO/COR, in writing, of any changes in access requirements for its personnel no later than one (1) day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to another contract. The Contractor's Program Manager is responsible for the completion and timely submission to the CO/COR of the CF-242 "*Separation Procedures for Contractor*

Employee" for all departing contract personnel. Contractor shall also provide OIT/Information Security Branch (ISB) the following information on behalf of their personnel to telephone number (b) (6) [redacted] or fax the below information to (b) (6) [redacted]

Full Name
Social Security Number
Effective Date
Reason for Change

f. "DHS/OS/SSPD CONCURS AND APPROVES THE 'NEED-TO-KNOW' AT THE SCI LEVEL /NON-SCI LEVEL" TOP SECRET CLEARANCES: ACCESS TO INTELLIGENCE INFORMATION REQUIRES A FINAL U.S. GORVERNEMENT CLEARANCE. SUBCONTRACTING: SUBCONTRACTING REQUIRES PRIOR APPROVAL OF THE GCA. BRIEFINGS: Special briefings and procedures ARE REQUIRED. THE DSS (CSO) DOES NOT CONDUCT INSPECTIONS FOR SENSITIVE COMPARTMENTED INFORMATION 9SCI0, BUT MUST INSPECT NON-SCI INTELLIGENCE MATERIAL THE CONTRACTOR PROSESSES."

9.1.2. Security Documentation

The Contractor shall provide the COR with the following information within three (3) business days of each employee's successful adjudication of the BI or the issuance of the Interim Clearance:

a. A signed and dated statement from each Contractor employee that he/she has received, read, and understands the CBP requirements contained in the DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*; Management Directive (MD) 4300.1 *Information Technology Systems Security*; and the DHS 4300A *Sensitive Systems Handbook*:

"I, [insert name of employee]_____, have read and understand the contents of the: DHS MD 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*; DHS MD 4300.1 *Information Technology Systems Security*; and The DHS *Sensitive Systems Handbook* 4300A Sensitive Systems Handbook.

I understand that there could be an impact to the CBP systems, as well as other consequences, for not following the requirements of these security documents."

9.1.3. Security Requirements for Unclassified Information Technology Resources, HSAR 3052.204-70

The Contractor shall contact the COR for security matters. The COR will provide assistance and direction.

(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 sixty (60) 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 six (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.

9.1.4 Contractor Employee Access, HSAR 3052.204-71

(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.

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, add the following paragraphs:

(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.

9.1.5 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 Authorizing Officials (AOs) or by the official designated by the AO to have signatory authority.

9.2 Web Services

The system or application delivered by the vendor must provide Web Services functionality (in accordance with Federal security and privacy guidelines) that will allow for the exchange or sharing of functions and data within their system to and from DHS and CBP owned or contracted systems. CBP and the vendor will define the data needed to be exchanged or shared, the data file formats, the web services exchange mechanism and Application Program Interfaces (APIs) and architecture, as well as the periodicity (up to and including instantaneous, bi-directional data feeds between the vendor system and CBP systems or databases).

Data input into vendor systems is owned by DHS and CBP and must be delivered upon demand or at the termination of the contract, in an electronic file format specified by CBP. Upon the completion or termination of a contract and delivery of DHS'/CBP's data as described, vendors are required to destroy their local copies of the data upon approval by CBP.

Additional details regarding web services requirements are noted in section 4.8.

9.3. Security Authorization (SA)

Security Authorization (SA) consists of important activities that support a risk management process and are an integral part of an agency's information security program. The security authorization process is designed to ensure that an information system will operate with the appropriate management review, that there is ongoing monitoring of security controls, and that reauthorization occurs periodically.

The Contractor must conduct and complete all required procedures and documentation resulting in a successful SA, formerly Certification and Accreditation (C&A) of their system or systems by the Department of Homeland Security (DHS) and/or US Customs and Border Protection (CBP), whether hosted internally within DHS or CBP networks or hosted externally. Prior SA for/by another private, Federal, State, or Local entity does not constitute completion of this requirement. Prior SA by DHS or CBP may also not constitute completion of this requirement, given that each implementation of a system can and does change SA factors such as accreditation boundaries which may trigger the need for a new, successful SA. The Contractor must adhere to contract deliverable requirements that require all deliverables to be submitted in a timely manner. All deliverables are subject to management approval prior to acceptance.

The Contractor shall meet the requirements of:

- DHS Sensitive Systems Policy Directive 4300A, Information Technology Security Program;

- CBP Information Systems Security Policies and Procedures Handbook, HR 1400-05D; and
- Guidance provided in Section 9.4.2

to provide the following:

9.3.1. Initiation

9.3.1.1 Information System Description

- Confirm that the information system has been completely and accurately described and documented.

9.3.1.2. Security Categorization

- Confirm that the security category of the information system has been determined and documented.

9.3.1.3 Privacy Threshold Analysis

- Review and document attribute of personally identifiable information collected by the information system.
- Identify and document why the data is being collected, the intended use of the information, with whom the information will be shared, opportunities for consent and how consent is granted, and how the information will be secured.

9.3.1.4. E-Authentication

- Document risk ratings (High, Moderate, Low) for each identified transaction based on impact of unauthorized access to reputation, health and safety, productivity and performance, administrative action, regulatory and legislative compliance, finance, and fines and legal penalties.
- Assign assurance level to information system based on M-04-04 guidance, and validate that the information system has achieved the required assurance level.

9.3.1.5 Security Plan

- Confirm that the system description including purpose, mission, system type (major application, general support system, or minor application), system boundary, users, type of information, information classification, system components (software and hardware), environment, interconnections, etc. have been identified.

9.3.1.6. Contingency Plan

- Document system description, line of succession, and contingency responsibilities.
- Document notification/activation phase procedures to include notification procedures, damage, assessment, and plan activation.
- Document recovery/reconstitution phases activities to include the sequence of recovery events and recovery procedures, and the necessary activities to return to original or new facility for normal operations.

9.3.2 Assessment

9.3.2.1. Security Control Assessment

- Assess the management, operational and technical security controls protecting and in the information system (including hardware, software, firmware, and surrounding environment) using methods and procedures, documentation and supporting materials necessary for the assessment of the security controls.

9.3.2.2. Security Testing and Evaluation (ST&E)

- Participate in the ST&E Kickoff meeting.
- Review and agree to the ST&E Plan.
- Allow the ST&E Team access to Contractor facilities to conduct security testing. The ST&E team will ask Contractor personnel to perform testing on their systems; if Contractor personnel believe that a particular test will cause a problem with the system, the notification shall be provided in advance to the ST&E team and arrangements will be made.

9.3.2.3. Contingency Plan Testing

- Establish and document plans for contingency testing to include system recovery on an alternate platform from backup media, coordination among recovery teams, internal and external connectivity, system performance using alternate equipment, restoration of normal operations, and notification procedures.

- Assist in performing tabletop and/or functional contingency exercises.

9.3.2.4. Disaster Recovery Strategies

- Review policy and procedures, as well as existing security documentation to determine the level of effort and resources required to develop the contingency plan.
- Identify and document preventive controls (e.g., UPS, generators, fire detection and suppression systems, water sensors, etc.)
- Identify and document backup procedures, offsite storage locations, alternative processing sites, equipment replacement strategies and/or existing compatible equipment, and roles and responsibilities for recovery teams.

9.3.2.5. Disaster Recovery Planning & Testing – Hardware

If the CBP 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 sixteen (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.

9.4. Continuous Monitoring (CM)

9.4.1 Document Information System Changes

- Using established CBP configuration management and control procedures, document proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment).

9.4.2. Security Impact Analysis

- Analyze the proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment) to determine the security impact of such changes.

9.4.3. Annual Security Control Assessment

- Assess the CBP agreed-upon set of security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Review previous assessments of security controls, including findings, results, and evidence.
- Identify any deviations or vulnerabilities, describing the vulnerability, the applicable threat agent / threat source capable of exploiting the vulnerability, the likelihood / occurrence of the exploit, the impact if exploited, and an assessment of the risk.
- Document any issues or vulnerabilities using the Plan of Action and Milestones (POA&M) guidance provided during the Security Authorization process.

9.4.4. Security Documentation Review/Update

- Update the security documentation based on changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.

9.4.5. Plan of Action and Milestones (POA&M) Update

- Update the POA&M Plan based on the documented changes to the information system (including hardware, software, firmware, and surrounding environment), and the results of the continuous monitoring process.

9.5. Deliverables, References, Resources, and Monitoring

9.5.1. Deliverables

Deliverable	Description	Delivery/ Frequency	Submit To
Security Authorization Activities will include, but may not be limited to the following:			
FIPS 199	The data in all systems must be categorized in accordance with FIPS-199, *Standards for Security Categorization of Federal Information and Information Systems* to determine the sensitivity level for Confidentiality, Integrity, and Availability. This categorization serves as the basis for determining security requirements for the system.	TBD Security Assessment Schedule	CO/COR
E-Authentication	An E-Authentication assessment is required to determine access control requirements for certain systems.	TBD Security Assessment Schedule	CO/COR
Privacy Threshold Analysis (PTA)	The Privacy Threshold Analysis (PTA) is used to determine whether the system is a Privacy Sensitive System that contains Personally Identifiable Information (PII) and whether a Privacy Impact Assessment (PIA) or System of Records Notice (SORN) is needed.	TBD Security Assessment Schedule	CO/COR
Risk Assessment (RA)	A Risk Assessment (RA) is used to identify the level of protection that is needed for a system.	TBD Security Assessment Schedule	CO/COR
Requirements Traceability Matrix (RTM)	A Requirements Traceability Matrix (RTM) is a document use to identify the criteria required to conduct testing to ensure that the controls for the system are implemented properly and are operating as intended.	TBD Security Assessment Schedule	CO/COR
Security Plan	The Security Plan is the definitive reference document for security information pertaining to a specific information system.	TBD Security Assessment Schedule	CO/COR
Contingency Plan (CP)	The Contingency Plan (CP) must document actions to be taken in the event that a system becomes unavailable due to unplanned circumstances.	TBD Security Assessment Schedule	CO/COR
Contingency Plan Test (CPT)	The purpose of a Contingency Plan Test (CPT) is to ensure that the system can be recovered and key personnel know and can perform their roles.	TBD Security Assessment Schedule	CO/COR
Plan of Action & Milestones (POA&Ms)	Plans of Action and Milestones (POA&Ms) are used to document remediation activities for resolving weaknesses in a system identified from any source.	TBD Security Assessment Schedule	CO/COR
Continuous Monitoring Activities will include, but may not be limited to the following:			

Deliverable	Description	Delivery/ Frequency	Submit To
Plan of Action & Milestones (POA&M) Plan	A living document that continues to provide the measures that have been implemented or are planned to correct any deficiencies noted during the security assessment.	TBD Security Assessment Schedule	CO/COR
Security Authorization Documentation Review	Review and updating, as necessary of security documentation.	TBD Security Assessment Schedule	CO/COR
Annual Control Assessments	Annual assessment of security controls.	TBD Security Assessment Schedule	CO/COR
Contingency Plan / Contingency Plan Tests	Annual Contingency Plan Test and Plan Updates	TBD Security Assessment Schedule	CO/COR
Vulnerability Assessment	Monthly scanning of systems and providing resulting audit reports.	TBD Security Assessment Schedule	CO/COR

9.5.2. References

The Contractor shall be familiar with all of the references below which provide policy, regulations and guidance that have a bearing on the Security Authorization Process.

Legislation

- Federal Information Security Management Act of 2002 (FISMA) (Title III of the E-Government Act, Public Law (PL) 107-347)
- Privacy Act of 1974, 5 U.S.C. § 552a
- OMB Circular A-123 – Management's Responsibility for Internal Control
- OMB Circular A-127 – Financial Management Systems
- OMB Circular A-130 – Management of Federal Information Resources
- Computer Fraud and Abuse Act of 1986, PL 99-474, 18 U.S.C. § 1030
- Computer Security Act of 1987, PL 100-235
- Paperwork Reduction Act, 44 U.S.C. § 3501, *et. seq.*
- Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended

Policies, Directives, Instructions

- DHS *Sensitive Systems Policy* Directive 4300A
- DHS 4300A *Sensitive Systems Policy Handbook*

Standards

- Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*

Guidelines

- NIST Special Publications (SPs) in the 800 series, but especially:
  - SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*
  - SP 800-30, *Guide for Conducting Risk Assessments (Draft)*
  - SP 800-34, *Contingency Planning Guide for Federal Information Systems*
  - SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

- SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*
- SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*
- SP 800 60, *Guide for Mapping Types of Information and Information Systems to Security Categories: Volume 1- Guide Volume, Volume 2 - Appendices*

The above references can be found at:

Office of Management and Budget (OMB) - http://www.whitehouse.gov/omb/circulars_default

Other Legislation – *can be found by searching on the title*

NIST – http://csrc.nist.gov/publications/PubsSPs.html

DHS/CBP – *have been included as an attachment*

9.5.3. 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.

9.5.4. Common Security Configuration

9.5.4.1. Common Security Configuration Clause, OMB-M-07-18 FDCC/

In acquiring information technology, Contractors 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.

9.5.5 Monitoring/Reviewing Contractor Security Requirements

9.5.5.1. 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.

"All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD140-01, *Information Technology Systems Security and 4300A Sensitive Systems Handbook*."

Attachment 2 – Fixed Pricing Matrix

Fixed Price for Security Authorization/Reauthorization and Continuous Monitoring

Cost Element	Base	Option 1	Option 2	Option 3	Option 4
Security Authoization / Reauthorization	(b) (4) [redacted]				
Continuous Monitoring					

Fixed Prices for Assessments to be Automated

Task	Base	Option 1	Option 2	Option 3	Option 4
Automation, Job Knowledge Test	(b) (4) [redacted]				
Automation, Logical Reasoning Test					
Automation, Writing Test					
Automation, Writing Sample Test					
Automation, Job Simulation					
Automation, Biodata Test					
Automation, Practice Test					

Fixed Prices for Mobile Testing Sites

International Test Sites	**Base**	**Option 1**	**Option 2**	**Option 3**	**Option 4**
Location	**Cost Factor**	**Cost Factor**	**Cost Factor**	**Cost Factor**	**Cost Factor**
Hong Kong, China	(b) (4) [redacted]				
Paris, France					
Dublin, Ireland					
Barcelona, Spain					
Naples, Italy					
Montreal, Canada					
Ottawa, Canada					
Toronto, Canada					
Vancouver, Canada					
Outside 120 miles					
Within 120 miles					

Fixed Price for Test Sessions

Test Sessions	Base	Option 1	Option 2	Option 3	Option 4
Test Battery (60 minute session)	(b) (4)				
Test Battery (60 minute session) - No Show/Late Cancel					
Test Battery (90 minute session)					
Test Battery (90 minute session) - No Show/Late Cancel					
Test Battery (120 minute session)					
Test Battery (120 minute session) - No Show/Late Cancel					
Test Battery (150 minute session)					
Test Battery (150 minute session) - No Show/Late Cancel					
Test Battery (180 minute session)					
Test Battery (180 minute session) - No Show/Late Cancel					
Test Battery (210 minute session)					
Test Battery (210 minute session) - No Show/Late Cancel					
Test Battery (240 minute session)					
Test Battery (240 minute session) - No Show/Late Cancel					
Test Battery (270 minute session)					
Test Battery (270 minute session) - No Show/Late Cancel					
Test Battery (300 minute session)					
Test Battery (300 minute session) - No Show/Late Cancel					
Test Battery (330 minute session)					
Test Battery (330 minute session) - No Show/Late Cancel					
Test Battery (360 minute session)					
Test Battery (360 minute session) - No Show/Late Cancel					
Test Battery (390 minute session)					
Test Battery (390 minute session) - No Show/Late Cancel					
Test Battery (420 minute session)					
Test Battery (420 minute session) - No Show/Late Cancel					
Test Battery (480 minute session)					
Test Battery (480 minute session) - No Show/Late Cancel					