

2. AMENDMENT/MODIFICATION NO. P00001	3. EFF. DATE 08/19/2010	4. REQUISITION/PURCHASE REQ. NO. 0020053769	5. PROJECT NO. (If applicable)
---	----------------------------	--	--------------------------------

6. ISSUED BY DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229	7. ADMINISTERED BY (If other than Item 6) DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229
---	--

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and Zip Code) BART & ASSOCIATES INC 8300 GREENSBORO DR (STE 900) MCLEAN VA 22102-3640	9A. AMENDMENT OF SOLICITATION NO. 9B. DATED (SEE ITEM 11) 10A. MODIFICATION OF CONTRACT/ORDER NO. / HSBP1010F00176 10B. DATED (SEE ITEM 13) 05/02/2010
--	--

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended, is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

A.	THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
B.	THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (Such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103 (b).
X	THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 43.103(A)(3), BILATERAL AGREEMENT BETWEEN BOTH PARTIES
D.	OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not is required to sign this document and return _____ copies to issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)
The purpose of this modification P00001 to HSBP1010F00176 is to accomplish the following:

1. Additional funding to support ePassport Project Support, ESTA Fee Website, Tecs Mod CSIS Development, WLUS O&M, TT GOES Seamless TvI, and CBP-TSA APIS.
- Line Items 220-290 have been added in the amount of \$2,402,559.32 see addendum for details.
2. Adding additional contract clauses see attached.
3. Adding the Statement of Work see attached.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print) (b) (6)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) HERMAN T. SHIVERS Contracting Officer	
15C. DATE SIGNED 8/20/10	16B. UNITED STATES OF AMERICA BY (b) (6) (Signature of Contracting Officer)	16C. DATE SIGNED 8/19/2010

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT			1. CONTRACT ID CODE	PAGE OF PAGES 1 2
2. AMENDMENT/MODIFICATION NO. P00001	3. EFF. DATE 08/19/2010	4. REQUISITION/PURCHASE REQ. NO. 0020053769	5. PROJECT NO. (If applicable)	
6. ISSUED BY DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229	CODE 70050800	7. ADMINISTERED BY (If other than Item 6) DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229		
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and Zip Code) BART & ASSOCIATES INC 8300 GREENSBORO DR (STE 900) MCLEAN VA 22102-3640 CODE 603180985 FACILITY CODE		9A. AMENDMENT OF SOLICITATION NO.		
		9B. DATED (SEE ITEM 11)		
		10A. MODIFICATION OF CONTRACT/ORDER NO. / HSBP1010F00176		
		10B. DATED (SEE ITEM 13) 05/02/2010		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended, is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

<input type="checkbox"/>	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
<input type="checkbox"/>	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (Such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103 (b).
<input checked="" type="checkbox"/>	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 43.103(A)(3), BILATERAL AGREEMENT BETWEEN BOTH PARTIES
<input type="checkbox"/>	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not is required to sign this document and return _____ copies to issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification P00001 to HSBP1010F00176 is to accomplish the following:

1. Additional funding to support ePassport Project Support, ESTA Fee Website, Tecs Mod CSIS Development, WLUS O&M, TT GOES Seamless Tvl, and CBP-TSA APIS.

Line Items 220-290 have been added in the amount of \$2,402,559.32 see addendum for details.

2. Adding additional contract clauses see attached.

3. Adding the Statement of Work see attached.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) HERMAN T. SHIVERS Contracting Officer	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY (b) (6)(b) (6) (Signature of Contracting Officer)	16C. DATE SIGNED 8/19/2010

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT - Continuation			1. TRACT ID CODE	
2. AMENDMENT/MODIFICATION NO. P00001	3. EFF. DATE 08/19/2010	4. REQUISITION/PURCHASE REQ. NO. 0020053769	PAGE OF 2	PAGES 2

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

4. Adding the Labor Categories and Rates Table see attached.

5. The task order value is changed from \$49,999,626.33 increased by \$2,402,559.32 for a new task order value of \$52,402,185.65.

The ending period of performance is for this task order remains at 01 February 2011.

All other terms and conditions of this task order remain unchanged.

**ATTACHMENT INFORMATION
FOR
AWARD/ORDER/IA MODIFICATION: HSBP1010F00176P00001**

I.1 PRICING PROVISIONS FOR TASK ORDER OR BLANKET PURCHASE AGREEMENT ISSUED UNDER A FEDERAL SUPPLY SCHEDULE (JUN 2005)

"This task order/Blanket Purchase Agreement (BPA) is placed under the terms and conditions of the GSA Federal Supply Schedule contract identified herein. The contractor warrants that, throughout performance, the prices charged the Government shall be as low as, or lower than, those charged the contractor's most favored customers and that the Government shall never be charged more under this order than the offeror/contractor's current GSA schedule rates, or the rates contained in the task order schedule, whichever are lower.

If this order contains options for additional periods of performance, U.S. Customs & Border Protection (CBP) will invoke the option only if the offeror/contractor maintains a current GSA schedule. Unilateral options will not be invoked if the rates indicated in the task order schedule for the option are higher than current GSA schedule rates, but may be invoked bilaterally at the offeror/contractor's current GSA rates. The contractor shall provide notice to the Government of any proposed and/or approved change to the GSA schedule rates. Failure to comply with the provisions of this price warranty may be cause for termination of the order and the offeror/contractor may be required to adjust their billing and/or reimburse the Government for any charges invoiced in violation of the price warranty."

[End of Clause]

I.2 SPECIFICATIONS, STATEMENT OF WORK, OR STATEMENT OF OBJECTIVES ATTACHED (MAR 2003)

The Specifications, Statement of Work, or Statement of Objectives which describe the work to be performed hereunder, although attached, is incorporated and made a part of this document with the same force and effect of "specifications" as described in the clause, Order of Precedence, FAR 52.215-8, incorporated by herein by reference.

[End of Clause]

I.3 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)

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

[End of Clause]

I.4 SUBMISSION OF INVOICES (JUN 2009)

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

1. Payment Center:

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

OR as an alternative:

Email: cbpinvoices@dhs.gov

Note – Only for awards with payment terms less than net 30:

The Subject line for all Emailed invoices to the National Finance Center must include the text
“Per CBP, Net [state # days] Invoice.”

2. Contracting Officer's Technical Representative (fill in at time of award):

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

OR as an alternative:

Email: (b) (6)

3. Contracting Officer (or Contract Administrator)(fill in at time of award):

DHS/U.S. Customs and Border Protection
Attention: HERMAN T. SHIVERS

OR as an alternative:

Email: (b) (6)

To constitute a proper invoice, the invoice shall include all the items required by Federal Acquisition Regulation (FAR) 32.905.

[End of Clause]

I.5 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

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

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

[End of Clause]

I.6 SECURITY PROCEDURES (OCT 2009)

A. Controls

1. The Contractor shall comply with the U.S. Customs and Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.
2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor shall comply with all security policies contained in CBP Handbook 1400-05C, Information Systems Security Policies and Procedures Handbook.
3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Management Directive (MD) 4300.1, Information Technology Systems Security Program and DHS 4300A, Sensitive Systems Handbook.
4. All Contractor employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Technical Representative (COTR). The COTR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Internal Affairs, Security Management Division (IA/SMD) should be notified if building access is revoked.
5. All Contractor employees must be registered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COTR. The Contractor shall provide timely start information to the CO/COTR or designated government personnel to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COTR or designated government personnel shall provide the Contractor with instructions for receipt of CTS registration information. Additionally, the CO/COTR shall immediately notify IA/SMD of the contractor's departure/separation.
6. The Contractor shall provide employee departure/separation date and reason for leaving to the CO/COTR in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the Contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

B. Security Background Investigation Requirements

1. In accordance with DHS Management Directive (MD) 11055, Suitability Screening Requirements for Contractors, Part VI, Policy and Procedures, Section E, Citizenship and Residency Requirements, contractor employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status. A waiver may be granted, as outlined in MD 11055, Part VI, Section M (1).
2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with MD 11055, Part VI, Section E (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in MD 11055, Part VI, Section M (2)
3. Provided the requirements of DHS MD 11055 are met as outlined in paragraph 1, above, contractor employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the employee's access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor employee's life, including employment, education, residences, police and court inquires, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPI).
4. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated BI or SSBI that meets federal investigation standards.. For employee candidates needing a BI for this contract, the Contractor shall require the applicable employees to submit information and documentation requested by CBP to initiate the BI process.
5. Background Investigation information and documentation is usually submitted by completion of standard federal and agency forms such as Questionnaire for Public Trust and Selected Positions or Questionnaire for National Security Positions; Fingerprint Chart; Fair Credit Reporting Act (FCRA) form; Criminal History Request form; and

Financial Disclosure form. These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.

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

C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.
2. The CO/COTR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.
3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.
4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.
5. Upon completion of this contract, the Contractor shall return all sensitive information used in the performance of the contract to the CO/COTR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

D. Notification of Contractor Employee Changes

1. The Contractor shall notify the CO/COTR via phone, facsimile, or electronic transmission, immediately after a personnel change become known or no later than five (5) business days prior to departure of the employee. Telephone notifications must be immediately followed up in writing. Contractor's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.
2. The Contractor shall notify the CO/COTR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. The CO/COTR will notify the Office of Information and Technology (OIT) Information Systems Security Branch (ISSB) of the proposed change. If a security clearance is required, the CO/COTR will notify IA/SMD.

E. Non-Disclosure Agreements

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

[End of Clause]

I.7 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]

I.8 TRAVEL COSTS (AUG 2008)

Costs for transportation, lodging, meals, and incidental expenses shall be reimbursed in accordance with Federal Acquisition Regulation (FAR) Subsection 31.205-46 and acceptable accounting procedures.

If it becomes necessary for the contractor to use the higher actual expense method repetitively or on a continuing basis in a particular area (see FAR 31.205-46(3)(iii)), the contractor must obtain advance approval from the contracting officer and comply with all requirements for justifications and documentation set forth in FAR Subsection 31.205-46 for allowability of travel costs.

As provided in FAR 31.205-46(a)(5), the Contracting Officer may consider an advance agreement (see FAR 31.109) with the contractor to avoid confusion in the treatment of costs anticipated to be incurred in unusual or special travel situations. The advance agreement shall be incorporated in the contract.

[End of Clause]

I.9 POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE (JUL 2010)

a. Contractor Performance Evaluation

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

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

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

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

b. Primary and Alternate Corporate Senior Contractor Representatives

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

c. Electronic access to contractor Performance Evaluations

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

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

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

[End of Clause]

I.10 HOLIDAYS AND ADMINISTRATIVE LEAVE (MAR 2003)

U.S. Customs & Border Protection (CBP) personnel observe the following days as holidays:

- | | |
|-------------------------------|------------------|
| New Year's Day | Labor Day |
| Martin Luther King's Birthday | Columbus Day |
| President's Day | Veteran's Day |
| Memorial Day | Thanksgiving Day |
| Independence Day | Christmas Day |

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

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

Except for designated around-the-clock or emergency operations, contractor personnel will not be able to perform on site under this contract with CBP on holidays set forth above. The contractor will not charge any holiday as a direct charge to the contract. In the event Contractor personnel work during a holiday other than those above, no form of holiday or other premium compensation will be reimbursed as either a direct or indirect cost. However, this does not preclude reimbursement for authorized overtime work.

In the event CBP grants administrative leave to its Government employees, at the site, on-site contractor personnel shall also be dismissed if the site is being closed. However, the Contractor shall continue to provide sufficient personnel to perform around-the-clock requirements of critical efforts already in progress or scheduled and shall be guided by the instructions issued by the Contracting Officer or her/his duly appointed representative. In each instance when the site is closed to Contractor personnel as a result of inclement weather, potentially hazardous conditions, explosions, or other special circumstances; the

Contractor will direct its staff as necessary to take actions such as reporting to its own site(s) or taking appropriate leave consistent with its policies. The cost of salaries and wages to the Contractor for the period of any such site closure are a reimbursable item of direct cost under the contract for employees whose regular time is normally a direct charge if they continue to perform contract work; otherwise, costs incurred because of site closure are reimbursable as indirect cost in accordance with the Contractor's established accounting policy.

[End of Clause]

I.11 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 .

(End of clause)

I.12 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)

I.13 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	WHTI VPC O&M - Labor	1.000	AU	(b)	(4)
10 cont.	Internal Tracking 50-1 = (b) (4) 50-4 = (b) (4)				
20	WHTI EDL	1.000	AU	(b)	(4)
30	WHTI Trusted Travel Enrollment Support	1.000	AU		
40	WHTI QA Support - Labor	1.000	AU		
50	D TOPS O&M	1.000	AU		
60	TECS MOD Dev SI	1.000	AU		
70	TECS MOD O&M	1.000	AU		
80	TECS MOD HPPQ Dev	1.000	AU		
90	TECS MOD TVL DOCS DEV	1.000	AU	(b)	(4)
100	TECS MOD Project Support	1.000	AU		
110	WLUS Labor	1.000	AU		
120	Enforcement O&M	1.000	AU		
130	Enforcement NCIC	1.000	AU	(b)	(4)
140	Enforcement O&M USV	1.000	AU		
140 cont.	Internal Tracking 50-2 = (b) (4) 50-3 = (b) (4) 50-9 = (b) (4)				
150	Enforcement O&M APIS	1.000	AU		

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
150 cont.	Internal tracking 10-1 = (b) (4) 10-2 = (b) (4) 10-3 = (b) (4)			(b)	(4)
160	Primary/Secondary Ops	1.000	AU	(b)	(4)
160 cont.	Internal Tracking 30-2 = (b) (4) 30-3 = (b) (4) 30-4 = (b) (4) 30-5 = (b) (4) 30-6 = (b) (4)			(b)	(4)
170	Enforcement O&M TPAC	1.000	AU	(b)	(4)
180	Enforcement Travel	1.000	AU	(b)	(4)
190	WHTI Image Archiving	1.000	AU	(b)	(4)
200	WHTI ATS/L Inbound VPC (v5)	1.000	AU	(b)	(4)
210	PLOR Reporting Capability	1.000	AU	(b)	(4)
220	ePassport Project Support	1.000	AU	(b)	(4)
230	ESTA Fee Website	1.000	AU	(b)	(4)
240	WLUS O&M	1.000	AU	(b)	(4)
250	TT GOES Seamless Tvl	1.000	AU	(b)	(4)
260	ESTA Fee Website	1.000	AU	(b)	(4)
270	TECS Mod CSIS Development	1.000	AU	(b)	(4)
280	TECS Mod CSIS Development	1.000	AU	(b)	(4)
290	TSA-CBP	1.000	AU	(b)	(4)

Total Funded Value of Award:

\$52,402,185.65

I.14 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2525USCSGLCS0923050000Z00010400AP01 640502525	(b) (4)
20	6100.2525USCSGLCS0923050000Z00010400AP01 640402525	(b) (4)
30	6100.2525USCSGLCS0923050000Z00010400AP01 640602525	(b) (4)
40	6100.2525USCSGLCS0923050000Z63F10400AP01 640702525	(b) (4)
50	6100.2525USCSGLCS0923050000Z63F10400HQ01 IS4602525	(b) (4)
60	6999.3155USCSGLCS0923050200Z63F10166HQ01 IS4803155	(b) (4)
70	6100.2525USCSGLCS0923050000Z63F10166HQ01 IS4802525	(b) (4)
80	6999.3155USCSGLCS0923050200Z63F10166HQ01 IS4803155	(b) (4)
90	6999.3155USCSGLCS0923050200Z63F10166HQ01 IS4803155	(b) (4)
100	6100.2525USCSGLCS0923050200Z63F10166HQ01 IS4802525	(b) (4)
110	6100.2525USCSGLCS0923050000Z63F10166HQ01 IS4802525	(b) (4)
120	6100.2525USCSGLCS0923050000Z63F10400HQ01 IS4902525	(b) (4)
130	6100.2525USCSGLCS0923050000Z63F10166HQ01 IS4802525	(b) (4)
140	6100.2525USCSGLCS0923050000Z63F10400AP01 IS4502525	(b) (4)
150	6100.2525USCSGLCS0923050000Z63F10400HQ01 IS4102525	(b) (4)
160	6100.2525USCSGLCS0923050000Z63F10400HQ01 IS4302525	(b) (4)
170	6100.2525GLCS0923050000ZJ0109091R0HQ01 IS4502525	(b) (4)
180	6100.2525GLCS0923050000ZJ0109091R0HQ01 IS4502525	(b) (4)
190	6100.2525USCSGLCS0923050000Z00010400AP01 640502525	(b) (4)
200	6100.2525USCSGLCS0923050000Z00010400AP01 640502525	(b) (4)
210	6100.2525USCSGLCS0923050000Z00010400AP11 IU4702525	(b) (4)
220	6100.2525GLCS0923050000ZJ6N08081R0HQ01 IS4502525	(b) (4)
230	6100.2525USCSGLCS0923050000Z00010400AP01 IU4702525	(b) (4)
240	6100.2525GLCS0923050000ZJ2F08081R0HQ01 IU4702525	(b) (4)
250	6100.2525USCSGLCS0923050000Z00010400AP11 IU4702525	(b) (4)

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
260	6100.2525USCSGLCS0923050000Z00010400HQ01 IU4702525	(b) (4)
270	6999.3155USCSGLCS0923050000Z00009166HQ01 IS4803155	
280	6999.3155USCSGLCS0923050000Z00010166HQ01 IS4803155	
290	6100.2525GLCS0923050000ZJGZ10104M0HQ01 IU5012525	

I.15 DELIVERY SCHEDULE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 7400 Fullerton Road Springfield, VA 22153	10	1.000	05/02/2010
	20	1.000	05/02/2010
	30	1.000	05/02/2010
	40	1.000	05/02/2010
	50	1.000	05/02/2010
	60	1.000	05/02/2010
	70	1.000	03/01/2010
	80	1.000	03/01/2010
	90	1.000	03/01/2010
	100	1.000	03/01/2010
	110	1.000	03/01/2010
	120	1.000	03/01/2010
	130	1.000	03/01/2010
	140	1.000	03/01/2010
	150	1.000	03/01/2010
	160	1.000	03/01/2010
	170	1.000	03/01/2010
	180	1.000	03/01/2010
	190	1.000	04/01/2010
	200	1.000	04/01/2010
	210	1.000	05/01/2010
	220	1.000	02/01/2011
	230	1.000	02/01/2011
	240	1.000	02/01/2010
	250	1.000	02/01/2011
	260	1.000	02/01/2011
	270	1.000	02/01/2011
	280	1.000	09/01/2010
	290	1.000	02/01/2011

I.16 STATEMENT OF WORK

**Passenger Systems Program Office
Software Support Services**

Project Title

Passenger Systems Program Office (PSPO) Software Development, Operations and Maintenance, Project Support and Security.

Background

U.S. Customs and Border Protection is one of the Department of Homeland Security's largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the U.S. It also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws.

The OIT is responsible for planning, designing, developing, testing, implementing and maintaining computer applications that support missions of CBP and other agencies. PSPO is responsible for systems that support the CBP mission, especially processing travelers at the POEs. Listed below are broad program applications that are currently under the administrative control of PSPO. This listing is not all inclusive and is subject to additions and deletions as business needs change.

Internet Solutions

Global Online Enrollment System (GOES) and related Global Entry System capabilities
Decal & Transponder Procurement System (DTOPS)
Electronic System for Travel Authorization (ESTA)
eAPIS General Aviation
CBP Vetting

Primary & Secondary Operations

TPAC/Ten Print
US-VISIT O&M
Western Hemisphere Travel Initiative (WHTI) – Vehicle Primary Client (VPC)
WHTI – Project Support (includes VPC)
US Pedestrian
US Arrival
Combined Automated Operations System (CAOS)

TECS Operations & Maintenance

TECS Legacy & Modernization Operations & Maintenance
Watch List Update Service
Primary Lookout Over Ride (PLOR)
Private Aircraft Enforcement System (PBRs)
National Crime Information Center (NCIC)
National Law Enforcement Telecommunication System
Advanced Passenger Information System (APIS) and APIS Quick Query
Operations Support

TECS Modernization

Secondary Inspection
High Performance Primary query and Manifest management
Travel Documents and Encounter Management
Infrastructure Support including Enterprise Reporting
Project Management
Privacy and Security
Watch List Update Services
Architectural Support

Project Support and Security

Scope

Software Support Services

For the purposes of defining the scope of the categories of services to be acquired under this SOW, "software support services" are defined as the performance of those activities required to capture, analyze and manage requirements, design, develop and test new systems, update existing systems, and to maintain all software systems once placed into operation. This definition does not limit the type of software support services, which can be performed during the SOW period.

Software support services for the mainframe, client/server and web environments will be acquired under this SOW for the following categories:

System Design and Development - New requirements for automated systems or major enhancements to existing systems must be captured, analyzed and managed, designed, developed, tested and implemented in CBP operational environment, to include converting legacy applications, databases and data.

Maintenance - Systems maintenance needs to be performed to accommodate emergency repairs to operational programs, changes in technology or adjustments in user requirements in existing systems.

Project Support and Security – support services for all lifecycle stages including configuration management, 3rd tier help desk support, system access support, process improvement and security.

Architectural Oversight - PSPO requires support for both architecture and application operating/monitoring functions across PSPO projects.

PSPO shall be responsible for identifying, defining and managing the technical direction of the development of modifications to the existing software systems and maintenance.

PSPO uses a structured approach in the development of its systems. For purposes of this solicitation, a structured approach is defined as a specific set of tasks that have to be accomplished in order to develop and/or enhance a system.

The following describes various responsibilities in the structured systems development approach. Requirements shall generally consist of, but are not limited to the following representative tasks:

- Review and analyze user requirements
- Develop functional and design requirements
- Design and develop programs based on user and functional requirements
- Data and database conversion
- Develop Test Plans and test cases/scenarios
- Program and system testing
- Document all work in accordance with the CBP and DHS SELC
- Technical oversight and technical management.
- Configuration management
- Data quality
- Project planning and tracking
- Quality Assurance
- Requirements Management
- Risk Management
- Technical Documentation
- Audit Compliance
- Process Improvement
- Production Data Analysis.
- Integrating legacy and Commercial off-the-shelf (COTS) software
- Task Order work/implementation plan
- Software maintenance
- Regulatory compliance
- Migrating or converting mainframe applications to client/server or web applications

Operations and Maintenance

The Contractor shall provide technical support to resolve reported software problems to ensure optimal performance, as well as provide minor enhancements (minor enhancements include, but are not limited to, activities to existing passenger systems modules, such as modifying information on a passenger system screen page, modifying passenger systems report formats, etc.) As part of these activities, the Contractor shall perform analysis of reported software defects, and provide software modifications and minor enhancements as required. All changes to the system must go through development and testing before they are moved into production. The Contractor shall provide the Government with full documentation of all system changes and/or modifications to the system software in writing as required in the DHS/CBP Systems Engineering Life Cycle (SELC). The Contractor shall provide analysis and programming assistance to identify and resolve problems or inefficiencies in existing related databases, files, and operational online or batch programs. This assistance shall include, but is not limited to, problem analysis, systems analysis, systems integration analysis, program modifications, help screen changes, program rewrites, stored procedures or triggers, and database and data file modifications or conversions. The Government will furnish all related existing systems documentation to the Contractor as required. The Contractor shall provide CBP with full documentation of any and all system changes and/or modifications to the existing system software, as specified by the Government.

The contractor shall provide any and all operations and maintenance (O&M) solutions, processes, and procedures necessary to sustain systems within the DHS enterprise at the highest levels of service and availability consistent with cost, schedule, and performance objectives. These solutions may be required across the DHS infrastructure, to include, but not limited to, the following operational areas: DHS/CBP data center, help desk, network and security operations, and collaboration Services.

Project Support and Security

In support of Technical Integration, the Contractor shall provide support for the following task(s):

Project Support

Project coordination across PSPO and other entities

Provide for and facilitate coordination across PSPO and other entities within DHS and CBP

Project Office Processes

Work to standardize and improve PSPO system development and maintenance processes

Identify and incorporate best practices to improve project planning, scheduling, monitoring, and reporting

Project Tracking Oversight

Track accomplishments against estimates, commitments, and plans

Report and track project status against Work Breakdown Structure

Compare and track to plan throughout the project's life cycle to include scope, cost, and schedule

Program Office Database Management

Manage Risk, Action Items, and Lessons Learned databases

Configuration Management

Mitigate software to Systems Acceptance Testing (SAT)

Assist with issues related to production moves and OIT CCB change requests

Provide Dimensions (configuration management tool) assistance

Quality Assurance

Conduct audits on processes and products

Document audit issues, corrective actions, and discrepancies

Provide audit reports and manage all issues to closure

Provide software life cycle and exit gate support

Requirements Management

Develop requirements management standards and procedures

Coordinate requirements modeling efforts across all PSPO projects

Involve users in requirements modeling sessions

Mentor PSPO team members with requirements modeling techniques

Section 508 Compliance

Review all new public facing hardware and software applications for Section 508 compliance

Develop use cases for Section 508 testing

Technical Writing

Write, edit, and format technical documentation in accordance with PSPO and Systems Life Cycle documentation standards

Create complex technical drawings in Microsoft Visio

Create Microsoft PowerPoint presentations

Design and process Open House and project support materials, brochures, and flyers

WorkLenz support

Assist PSPO project managers and technical leads with information to be presented at the Program Management Reviews

Ticket Support and Resolution

Resolve or send production issues received via the CBP Help Desk to appropriate project team

TECS production Updates

Update TECS production tables as required by the project teams

User Access

Provide access to users in TECS
Create new user profile and group codes
Enter new transactions and coordinate changes with Systems Security

Production Management

Serve as liaison for all production reports
Provide oversight of all documentation stored in the Operations Run Manual Systems

System Support

Work closely with the Technical Support Team to resolve Remedy tickets and other issues in support of PSPO teams, to which provides access to all TECS environment regions for PSPO analysts and programmers.

Security

Provide the connection between IT security policies and systems

Develop security controls from policies (OMB, DHS, CBP) and requirements
Collaborate on the implementation of security controls
Help develop compensating controls when minimum mandated security requirements cannot be implemented
Document the overall security effort for compliance through certification and accreditation
Continuously monitor security posture of PSPO systems through regular testing and assessment
Obtain the Authority to Operate (ATO) letter
Support internal and external IT audit activities

Security Design and Analysis

Provide security design analyses and review for impact on Passenger Systems application and CBP network. Active participation in the security working group led by the Passenger Systems ISSM and coordinate with CBP ISSB regarding management, operational, and technical security issues affecting the Passenger Systems and CBP network. Provide security analysis of Passenger Systems and CBP network connections and interfaces. This may include development of Interconnection Security Agreement (ISA) documents and Memorandum of Understanding as necessary.

Certification & Accreditation

The Contractor shall review and develop Certification and Accreditation (C&A) documents to assess and reflect the changes in security posture of Passenger Systems. The development of C&A documents will utilize the DHS mandated C&A tool, Risk Management System, and will include, at minimum, a System Security Plan, Risk Assessment, Security Test Plan and Report, and Continuity of Operation Plan. The Contractor shall coordinate any activities necessary with CBP ISSB to ensure that the updated C&A follows and satisfies all requirements under CBP and DHS security policies and guidelines.

Security Test and Reports

The Contractor shall conduct security testing of new and updated CBP hardware/software affecting Passenger Systems or CBP network's security posture. A review of Passenger Systems security test reports will be reviewed and analyzed to ensure that adequate security controls are in place to protect the Passenger Systems and CBP network from unauthorized access via other IT systems. Any security issues shall be coordinated with the Passenger Systems ISSM and CBP ISSM to identify mitigating controls and Plan of Action and Milestones will be developed.

Architecture Oversight

Architecture work includes helping PSPO projects to align with CBP and DHS architecture guidelines as well as representing PSPO interests in meetings and working groups at CBP and DHS on architecture related issues. Operating/monitoring functions include proactive monitoring of application functions to avoid or correct issues at the earliest opportunity and to identify areas where PSPO applications can be improved to run more robustly and efficiently. The system operating/monitoring functions will be done in coordination with the Enterprise Data Management and Engineering (EDME) and (ENTS). The architecture and operating/monitoring functions complement each other and should be closely tied to ensure interaction of the functions.

Requirements

Software Development Requirements

The Contractor shall provide the requirements development. This will require the Contractor to identify eleven topics that must be addressed:

Developed Systems
Interfaces
Functional Capabilities
Performance Levels
Data Structures/Elements
Safety
Reliability
Security/Privacy
Quality
Constraints and Limitations
Operational and Maintenance Models.

The Contractor shall provide qualified technical and management personnel resources to accomplish the following tasks:

Perform user requirements analysis.
Perform system integration analysis.
Perform system design analysis.
Perform system construction.
Perform Project configuration and Technical compliance review.
Provide a technical lead to support the government Technical Lead/Program Manager in various Exit Gate reviews.
Develop and maintain requirements traceability matrix and risk database.
Participate in the creation of a Work Breakdown Structure (WBS).
Participate in the development of the Life Cycle tailoring document.
Modify and develop programs based on user requirements (analysis).
Provide all associated DHS/CBP System Engineering Life Cycle (SELC)-compliant documentation as required.
Provide all associated CBP Architecture Alignment and Assessment (AAA) compliant documentation as required.
Provide all associated DHS Alignments (Milestone Decision Points) compliant documentation as required.
Provide testing and SQA support as necessary to correct Test problem reports.
 Support testing and configuration management team in preparing for production implementation.
 Conduct or participate in technical reviews as requested.
 Operate and maintain the system.
 Provide analysis and programming assistance to identify and resolve problems or inefficiencies in existing related databases, files and operational on-line or batch programs.
 Provide assistance to include, but not be limited to, problem analysis, systems analysis, program modifications, changing help screens, rewriting programs, stored procedures or triggers, and database and data file modifications or conversions.
 Migrate system components from development to testing, and subsequently, to production environment.
 Provide full documentation of any systems changes and/or modifications to the existing systems software, as specified by the Government. All related existing systems documentation shall be furnished by the Government to the Contractor as required.
 Maintain system development documentation using the Government furnished document management system.
Prepare on-line systems help.

Operations and Maintenance Requirements

The Contractor shall provide qualified technical and management personnel resources to accomplish the following tasks:

Perform user requirements analysis.
Perform system integration analysis.
Participate in the creation of Work Breakdown Structure (WBS).
Modify and develop programs based on user requirements (analysis).
Provide development and integration testing and quality assurance support as necessary to correct Test problem reports
 Conduct or participate in technical reviews as requested.
 Operate and maintain the systems.
 Provide analysis and programming assistance to identify and resolve problems or inefficiencies in existing related databases, files and operational on-line or batch programs.

Provide assistance to include, but not be limited to, problem analysis, systems analysis, program modifications, changing help screens, rewriting programs, stored procedures or triggers, and database and data file modifications or conversions.

All changes to the system must go through development and testing before they are moved into production.

Provide full documentation of any systems changes and/or modifications to the existing systems software, as specified by the Government.

Respond to Help Desk tickets

Respond to Operational Problem Reports (OPR)

Modify and/or develop programs based on analysis of end-user evaluation of current system components

Provide programming support as necessary to correct operational problem reports

Test all modifications against external interfaces

Modify code and test applications in conjunction with other related development efforts.

Coordinate closely with Government Program Managers, Government employees, and other contractors to ensure success across projects.

Coordinate with the Office of Information Technology (OIT) to assist in meeting the CBP process, procedure, and policy requirements for accountable property.

Be proactive in recommending solutions as issues arise and play an active role in their resolution.

Support deployment to additional sites and upgrade existing sites, including travel, labor, and equipment; shall support all other deployment efforts as directed by the COTR.

Produce ad hoc reports as required.

Provide all associated requirement documentation.

Perform Project configuration management as requested by the Government in accordance with industry best practices.

Perform Project Technical compliance review as requested by the Government in accordance with industry best practices.

Participate with COTR, Project Leads, and Government Business Program Managers in various SELC-related phase gate reviews.

Develop and maintain requirements traceability matrix.

Support and maintain CBP Risk Management Plan.

Participate in the creation of Work Breakdown Structure (WBS).

Modify and develop programs based on user requirements (analysis).

Participate in staff meetings and generate periodic status reports as required.

Provide documentation and input to facilitate security certification.

Coordinate with the CBP Tivoli group to maintain remote connectivity between the Contractor's site and the CBP network, and coordinate with the Tivoli group to ensure maximum utilization of all Tivoli features and capabilities.

Provide 3rd tier Help Desk and Operations Support as requested.

Help Desk support shall be provided during core hours from 8 A.M. to 5 P.M. EST, Monday through Friday.

Outside core ours, on-call support shall be provided 24/7.

The Contractor must provide user status notification within four hours of notification by the Level 1 help desk.

Emergency Release Support.

Respond to OIT data calls for financial, budget and Task Order administrative information.

3P Dimensions tool for all projects.

Provide testing and Software Quality Assurance support as necessary to correct Test problem reports.

Support the PSPO Independent Test Team and Configuration management team in preparing for production implementation.

Participate in technical reviews as requested.

Maintain the system as requested by the Government.

Provide analysis and programming assistance to identify and resolve problems or inefficiencies in existing related databases, files and operation on-line or batch programs.

This assistance to include, but not limited to, problem analysis, systems analysis, program modifications, changing help screens, rewriting programs, stored procedures or triggers, and database and data file modifications or conversions.

All changes to the system must go through development and testing before they are moved into production.

All related existing systems documentation shall be furnished by the Government to the Contractor as required.

Provide full documentation of any systems changes and/or modifications to the existing systems software, as specified by the Government.

Project Support and Security Requirements

The Contractor shall provide qualified technical and management personnel resources to accomplish the aforementioned tasks. This will include, but not be limited to, performance of the following system development functions:

Assist Project configuration and Technical compliance review

Assist Technical Lead/Program manager in various Exit Gate reviews

- Oversee development and status of the requirements traceability matrix and risk database
- Participate in the creation of Work Breakdown schedule (WBS)
- Participate in the development of the Life Cycle tailoring document
- Participate in the development conduct and documentation of the security program and security requirements
- Provide the appropriate certification and accreditation support
- Conduct or participate in management and technical reviews as requested.

Architecture Oversight Requirements

The contractor shall provide qualified technical and management personnel resources to accomplish the following tasks:

- Represent PSPO interests in architecture projects at the CBP and DHS levels.
- Develop architecture standards for PSPO projects based on CPB standards.
- Assist the PSPO project teams with understanding and implementing the architecture standards.
- Ensure that PSPO projects follow the PSPO, CBP and DHS architecture guidelines.
- Develop and implement a monitoring process for PSPO projects that proactively assesses system status in production to provide early alerts for problems or potential problems. This will include trending of issues and recommendations for architecture guidelines and/or system changes to make them more robust, efficient and easy to monitor.
- Develop and implement an operational problem correction capability to include tracking of outstanding issues until resolved. Depending on the situation the problem may be corrected by the monitoring team, EDME, ENTS and/or the application team but will be tracked to completion by the monitoring team.
- Provide monitoring/operations support for all PSPO environments (mainframe, client server, web, etc.).
- Work with the project teams to build monitoring into the applications and determine what aspects require monitoring.
- Work cooperatively and interactively with EDME and ENTS to ensure efforts are complimentary. EDME and ENTS efforts will be leveraged to provide a comprehensive view for PSPO operations.
- Provide analytical support for monitoring issues to work with the project teams to identify how to improve performance.
- Provide an interactive link between architecture guidelines and monitoring results.
- Provide documentation and presentation support for architecture and monitoring tasks.

Program Deliverables

All deliverables shall be delivered in hardcopy and electronic format. The Contractor shall develop documentation in the Microsoft office suite product approved by the COTR. No other office automation product shall be used, unless approved by the Government.

Deliverable	Due Date
Project Orientation Briefing	Date of award + 3 days, NLT 14 days
Complete DHS/CBP/PSPO security package requirements for all Key Personnel & proposed staff	Date of award + 7 days
Schedule of Deliverables	10 days from award date
Status Report of Activities	By the 10 th of each month, submitted with the invoice.
DHS/CBP SELC-compliant documentation	In accordance with the approved Delivery Schedule
Project Management Plan	10 days from date of award
Ad Hoc Reports	In accordance with the approved Delivery Schedule
Invoicing, including status report detailing the work completed during each month	By the 10 th of each month
DHS IT Security Plan	30 days from date of award

All work is to be done in compliance with the CBP Enterprise Architect (EA) as defined by the EA Branch and within the technical environment identified in the original contract.

Schedule of Deliverables

The Contractor shall submit to the COTR, ten days after date of award, a schedule of deliverables. All documents shall be delivered in Microsoft Office (Word, Excel, and/or Access) format, as required to the Contracting Officer and to the COTR. All manuals and procedural reports shall be bound in loose-leaf, three-ring binders. Change pages shall be

provided for interim changes made to the documents, and incorporated into the electronic and hard copy versions to be provided to the COTR, consistent with the instructions above.

The COTR may approve the Contractor's submission, or may provide comments. The Contractor shall incorporate CBP comments on documentation and the revised documentation reissued within two weeks of their receipt. Once accepted by the COTR, these documents shall become the property of CBP and will be distributed without restriction to other CBP offices and their Contractors to provide information on the Port of Entry Support Services. The Contractor shall operate in strict accordance with their approved documentation, unless the COTR provides alternative directions.

Invoicing

The objective is to have an accounting process in which the accounting books can be closed in a reasonable timeframe. For this to happen, invoices as well as any changes to the invoices must be submitted in a timely manner. Adherence to the following shall be included in the Government's evaluation of the Contractor's Program Management Performance.

The Contractor shall invoice the Government monthly for services performed under each task order. Invoices shall be for services and other direct costs incurred against the task order during the previous month's period of performance. The period of performance shall begin on the first (1st) of the month and end on the last day of that month. Invoices shall be received by the tenth (10th) day of each month and include billable items for the previous month's period of performance.

Invoice Submission

The Contractor shall submit invoices in both hard copy and electronically, including all supporting documents. Invoices shall contain the following information:

Company name and address

Name and address of person to whom payment is to be sent, including Electronic Funds Transfer information, if applicable

Name, title, and phone number of person to notify in the event of defective invoices.

The period of performance being invoiced. This must include the beginning and end dates (dd/mm/yyyy format) of the calendar

Contract number

Task order number (or task order modification number)

Total value of task order (or task order modification value)

Task order Period of Performance

Invoice number

Date invoice issued

Travel and per diem for invoice period (with all receipts and trip reports for the period)

Monthly Tabulation as follows:

Monthly hours by labor category, and, broken out within each labor category, monthly hours by individual employee, per project.

Brief description of work performed by each employee

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

Invoices shall include subtotals for all ODCs and travel.

ODC Process

The Contractor shall acquire the COTR or their designee's approval on all ODCs prior to initiating any purchase and/or ODC expense, including travel.

Invoice Modification

The Contractor shall endeavor to ensure that all employee time sheet submissions and all purchases are accurate and valid, and as such, the invoices submitted to the Government should not require future changes. In the event that an error is made, the change shall be recorded and invoiced within 90 days of the last day of the month in which the labor was performed. In addition, any such adjustment will contain detailed documentation explaining the error and the time period during which it occurred. No changes will be accepted after 90 days of the end of the period of performance.

Invoice Delivery

The contractor shall submit invoices as follows:

Original invoice and one copy to the Contracting Officer's Technical Representative

(b) (6) COTR
Passenger Systems Program Office
U.S. Customs and Border Protection

7681 Boston Blvd. – NDC3
Springfield, VA 22153

(b) (6)

Simultaneously, one copy of the invoice shall be mailed to the National Finance Center at the following address:

DHS – U.S. Customs and Border Protection
National Finance Center
P.O. Box 68908
Indianapolis, IN 46268

Electronic copies of the invoices are also acceptable. Please email your invoice to both, cbpinvoices@dhs.gov and to

(b) (6)

Government-Furnished Equipment and Information

(a) The DHS/CBP intends to furnish only that equipment necessary for the Contractor to carry out its work efforts under this Work Statement at the government facility. This only includes desk, chair, desk phone, and desktop computer. While performing work under this Work Statement in DHS/CBP facilities, the Contractor may have the use of other normal office EIT devices, such as FAX machines (not classified), copiers, projectors, etc.

(b) Upon approval by the COTR, DHS/CBP will provide to the Contractor cell phone or other portable devices, such as Blackberries or other PDAs and laptops as required.

Place of Performance

Work under this task will be performed at DHS offices in Springfield or Tysons Corner, VA. Some local travel to various sites in the Washington, DC metropolitan area for meetings and briefings will be required. Travel to sites outside of the Washington, DC area will likely be required.

Period of Performance

The period of performance for this effort is a nine months from date of award.

Security

Security Background Data

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

The applicable Contractor employees shall not begin working under this Delivery Order until all security forms have been properly completed and submitted to CBP Security. All Contractor employees shall be required to wear identification badges when working in Government facilities.

Contractor personnel hired for work within the United States or its territories and possessions, and who require access to Department of Homeland Security (DHS) owned or controlled facilities, information systems, security items or products and/or sensitive but unclassified information shall be a U.S. citizen.

The following security-screening requirements apply to U.S. citizens hired as Contractor personnel. All personnel employed by the Contractor or responsible to the Contractor for the performance of work hereunder shall either currently possess or be able to favorably pass a full field five year employment background investigation. The Contractor shall submit within ten (10) working days after award of this Delivery Order, a list containing the full name, social security number, and date of birth of those people who claim to have 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 for all personnel. The information must be correct and be reviewed by a CBP Security Official for completeness. Normally, this shall consist of SF-85P, "Questionnaire for Public Trust Positions" or SF-86, "Questionnaire for Sensitive Positions (For National Security)" TDF 67-32.5, "U.S. CBP Authorization for Release of Information"; FD-258, "Fingerprint Chart"; and a Financial Statement.

Failure of any Contractor personnel to pass a background investigation means that the Contractor has failed to satisfy the contract's requirement to provide cleared personnel. The continuing failure to meet the requirement to provide cleared personnel is grounds for termination of the contract, unless cleared personnel are timely provided as replacements. Failure of the Contractor personnel to pass a background investigation shall be cause for the candidate's dismissal from the project and replacement by a similar and equally qualified candidate as determined and approved by the Contracting Officer. This policy also applies to any personnel hired as replacements during the term of this Delivery Order.

If the Contractor employee requires access to operational DHS/CBP systems or data to begin their work a final clearance must be approved by CBP IA prior to the Contractor employee beginning work. CBP IA estimates that completion of the investigation will take approximately ninety (90) to one hundred twenty (120) days from the date they receive the packet.

Notification of Personnel Changes

The Contractor shall notify the CBP Project Lead, COTR, and CO via phone, FAX, or electronic transmission, no later than ten workdays after any personnel changes occur. Written confirmation is required for phone notification. This includes, but is not limited to, resignations, terminations, and reassignments including to another Delivery Order or contract. For personnel changes on ADIS, the Contractor shall also provide the above notification to the US-VISIT Mission Operations Office.

The Contractor shall notify the CBP Office of Information and Technology (OIT) Information Systems Security Branch (ISSB) of any change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other contractors. The Contractor shall provide the following information to OIT ISSB at Tel. (703) 921-6116 and FAX (703) 921-6570:

Full Name
Social Security Number
Effective Date
Reason for Change

Separation Procedures

In accordance with CBP Directive Number 51715-0006, "Separation Procedures for Contractor Employees," the Contractor is responsible for ensuring that all separating employees complete relevant portions of the Contractor Employee Separation Clearance, CBP Form 242. This requirement covers all Contractor employees who depart while the Delivery Order is active (including resignation, termination, etc.) or upon final completion of the Delivery Order. The Contractor shall keep a record of all separating employees, measure employee turnover, and provide this information upon request. Failure of a Contractor to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports.

General Security Responsibilities During Performance

The Contractor shall follow the general procedures governing physical, environmental, and information security described in the various CBP regulations pertaining thereto, good business practices, and the specifications, directives, and manuals for conducting work to generate the products required under this Delivery Order. The COTR will monitor/review security practices at contractor sites.

All Contractor personnel shall be responsible for the physical security of their area and government furnished equipment (GFE) issued to them under the provisions of the Delivery Order.

The Contractor's personnel must have the appropriate security clearance and all information must be protected to the degree and extent required by local rules, regulations, and procedures.

Employment Eligibility

The Contractor shall agree that each employee working on this task order shall have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the government for acts and omissions of his own employees and for any subcontractor(s) and their employees.

Subject to existing law, regulations and/or other provisions of this contract, illegal or undocumented aliens shall not be employed by the Contractor, or with this contract. The Contractor shall ensure that this provision is expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

Disclosure of Information

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

During the course of this Delivery Order, the Contractor shall not use, disclose, or reproduce data, which bears a restrictive legend, other than as required in the performance of this task.

In performance of this Delivery Order, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor's responsible employees.

Each officer or employee of the Contractor or any of its subcontractors to whom any Government records may be made available or disclosed, shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C 641. That section provides, in pertinent part, that whoever knowingly converts to their use or the use of another, or without authority, sells, conveys, or disposes of any record of the United States or whoever receives the same with intent to convert it to their use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine up to \$10,000 or imprisoned up to ten years, or both.

Systems Life Cycle.

The Contractor shall be governed by and comply with the provisions of the DHS/CBP System Life Cycle Handbook (DHS AD 102.01 DHS SELC). Any Contractor-specific best practices recommendations will be incorporated in a tailoring of the CBP Systems Life Cycle Handbook. However, this action must be prior approved by the COTR.

Use of Worklenz Product for Reporting Purposes.

(a) The Contractor shall perform program and project planning and management duties to facilitate the development of the system and operational requirements for the task elements. This will include, but is not limited to the preparation of plans and schedules based on technical and project data; tracking program funds; scheduling and conducting technical and planning meetings; conducting project reviews; and preparing status reports. This includes entering program related information in CBP's WorkLenz tool.

(b) The WorkLenz tool is required to accomplish the following:
Manage CBP/CIO resources both effectively and efficiently from an enterprise-wide standpoint;
Plan the development of new investments and projects in support of agency goals and objectives;
Ensure that investment and projects are being managed within specified cost, schedule, and performance parameters;
Foster the development of effective corrective action plans when needed.

(c) Within 7 days of receiving a WorkLenz Confidentiality Agreement, Contractor must have signed agreements by its staff assigned to CBP to the confidentiality provisions imposed by the Worklenz licensor.

(d) The Contractor shall be familiar with this tool and enter, track and report associated contract activities, as directed by the Program Office Task Monitors or the COTR, within the WorkLenz tool. The Contractor shall update information at regular one week intervals to provide Senior CBP Management with clarity, insight and visibility into on-going IT projects and operations. If support is in WorkLenz, the Contractor will contact the Program Manager Task Monitors or the COTR directly, and will not attempt to seek support from the WorkLenz licensor directly.

Contracting Officer's Technical Representative (COTR)

Name: (b) (6)
Executive Director
Address: 7681 Boston Blvd., NDC3
Springfield, VA 22153
Tel. #: (b) (6)
Fax #: (b) (6)
Email: (b) (6)

Contract Administrator:

Name: (b) (6)
Program Control Office
Address: 7681 Boston Blvd, NDC3
Springfield, VA 22153
Tel. #: (b) (6)
Fax #: (b) (6)
Email: (b) (6)

DHS Clauses

EA (Enterprise Architecture) Compliance

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

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

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

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

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

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

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

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

OAST (Office on Accessible Systems and Technology) Compliance

DHS Accessibility Requirements (Section 508 Compliance)

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools.

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

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

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

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

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

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

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

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

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

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

ISO (Information Security) COMPLIANCE

Information Security Clause:

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

Interconnection Security Agreements

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

HSAR Clauses

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

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

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

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

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

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

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 6.1.1, October 31, 2008) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

HSAR 3052.204-71 Contractor Employee Access Clause

CONTRACTOR EMPLOYEE ACCESS (JUN 2006)

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

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of 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.

System Security documentation appropriate for the SELC status.

Security Certification/Accreditation

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

Disaster Recovery Planning & Testing – Hardware

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

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

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

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

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

Monitoring/reviewing contractor security requirements clause

Security Review and Reporting

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

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

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

OMB-M-07-18 FDCC/Common Security Configuration Clause

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

Engineering Platforms

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

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

ITP (Infrastructure Transformation Program) COMPLIANCE

CBP has submitting a data center transition strategy to DHS in December 2009. PSPO will follow the CBP Plan. This purchase order is for application maintenance and support for FY10 for systems critical to CBP operations. Although we understand the concern on data center transition plans, it is not appropriate to hold up work on maintaining critical applications pending data center transition plans

Help Desk and Operations Support

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

Interfacing

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

TRANSITION PLAN

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

Coordination with Government representatives

Review, evaluation and transition of current support services

Transition of historic data to new contractor system

Government-approved training and certification process

Transfer of all necessary business and/or technical documentation

Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.

Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance

Applicable debriefing and personnel out-processing procedures

ADDENDUM

1. 2. Line Item Titles for funding lines

Line Item	Description	Amount
220	ePassport Project Support	(b) (6)
230	ESTA Fee Website	
240	WLUS O&M	
250	TT GOES Seamless Tvl	
260	ESTA Fee Website	
270	TECS Mod CSIS Development	
280	TECS Mod CSIS Development	
290	TSA-CBP	
	Grand Total	

BART & ASSOCIATES, INC.

LABOR CATEGORIES AND RATES TABLE

HSBP1010F00176 Mod P00001

PERIOD OF PERFORMANCE: 02 MAY 2010 - 01 FEB 2011

Labor Category	On-Site	Off-Site
	Rate	Rate
Admin Assist II	(b) (6)	(b) (6)
Bus Sys Analyst	(b) (6)	(b) (6)
Database Admin I	(b) (6)	(b) (6)
Consult	(b) (6)	(b) (6)
ERP Consult	(b) (6)	(b) (6)
ERP Consult I	(b) (6)	(b) (6)
IS Tech Spec	(b) (6)	(b) (6)
Multi-Discp Proc Coord	(b) (6)	(b) (6)
Proc Improv Coord	(b) (6)	(b) (6)
Proj Plan Spec	(b) (6)	(b) (6)
QA Spec	(b) (6)	(b) (6)
Sr. ERP Consult	(b) (6)	(b) (6)
Sr. Funct Consult	(b) (6)	(b) (6)
Sr. Proc Improv Coord	(b) (6)	(b) (6)
Sr. QA Spec	(b) (6)	(b) (6)
Sr. Sys Analyst	(b) (6)	(b) (6)
Sys Analyst	(b) (6)	(b) (6)
Tech Manager	(b) (6)	(b) (6)
Tech Writer	(b) (6)	(b) (6)
	(b) (4)	(b) (4)
	(b) (4)	(b) (4)
	(b) (4)	(b) (4)