



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

PAGE OF PAGES

2 3

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

1. DATE OF ORDER  
09/30/2010

2. CONTRACT NO. (if any)  
HSHQDC06D00021

3. ORDER NO.  
HSBP1010J00840

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Accept
80	TT Labor	1.000	AU	(b) (4)	(b) (4)	
90	TT Labor	1.000	AU	(b) (4)	(b) (4)	
100	GE Kiosk Systems	38.000	EA	(b) (4)	(b) (4)	
110	KIS CBP Global Entry one year factory wa	1.000	AU	(b) (4)	(b) (4)	
120	Acapela Heather Voice Multimedia	38.000	EA	(b) (4)	(b) (4)	
130	Aware Runtime License and Annual Maint	38.000	EA	(b) (4)	(b) (4)	
140	TT Labor	1.000	AU	(b) (4)	(b) (4)	
150	Misc ODCs/Services	1.000	AU	(b) (4)	(b) (4)	
160	Misc SW/Maint	1.000	AU	(b) (4)	(b) (4)	
170	Dell 760 Optiplex	1.000	EA	(b) (4)	(b) (4)	
180	Travel	1.000	AU	(b) (4)	(b) (4)	
190	Misc Equipment	1.000	EA	(b) (4)	(b) (4)	
200	PALS Server	1.000	EA	(b) (4)	(b) (4)	
210	InstallShield 2011 Pro + Maint	1.000	EA	(b) (4)	(b) (4)	
220	Guardian Edge Encryption SW	4000.000	EA	(b) (4)	(b) (4)	
230	Guardian Edge Encryption SW for PALS Lap	2000.000	EA	(b) (4)	(b) (4)	
240	Toughbook CF-52ELNHQ2M	14.000	EA	(b) (4)	(b) (4)	

DATE OF ORDER 09/30/2010	CONTRACT NO. (if any) HSHQDC06D00021	ORDER NO. HSBP1010J00840	PAGE OF PAGES 3 3
-----------------------------	---	-----------------------------	----------------------

**Federal Tax Exempt ID:** (b) (4)

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

**NOTES:**

This Time and Material (T & M) Task Order HSBP1010J00840 is issued to CSC, against EAGLE Contract IDIQ HSHQDC06D00021. This requirement was generated by U.S. Customs and Border Protection (CBP) Office of Information and Technology (OIT), Passenger Systems Program Office (PSPO).

CSC proposal dated 17 September 2010 is incorporated by reference.

This task order also incorporates the attached Performance Work Statement (PWS) submitted by CSC on 17 September 2010, for the Trusted Traveler Program within CBP.

The period of performance of this task order is:

Base Period: September 30, 2010 through February 01, 2011 \$9,999,818.93

Option Period: February 02, 2011 through May 01, 2011 \$6,454,363.97

The ceiling price of the base \$9,999,918.93 has been fully funded. All labor rates provided are fixed unit prices with applicable discounts as cited and are in effect for this task order as the billing rates (see addendum Price-Ceiling Schedule for the base and option period).

FAR 52.232-7 is applicable. As authorized by FAR 52.232-7(a) (7), the withhold percent is changed to (b) (4).

Attached are additional DHS HSAR clauses.

The designated Contracting Officer's Technical Representative (COTR) for this task order is (b) (6).

Please submit all invoices to each of the following:

U.S. Customs and Border Protection  
Office of Information and Technology (OIT)  
Passenger Systems Program Office (PSPO)  
7681 Boston Blvd., (NDC 3 - 202)  
Springfield, VA 22153  
Tel: (b) (6)  
e-mail: (b) (6)

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

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA  
FOR  
DELIVERY ORDER: HSBP1010J00840**

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

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	TT Labor	1.000	AU	(b) (4)	(b) (4)
20	TT Labor	1.000	AU	(b) (4)	(b) (4)
30	TT Labor	1.000	AU	(b) (4)	(b) (4)
40	TT Labor	1.000	AU	(b) (4)	(b) (4)
50	TT Labor	1.000	AU	(b) (4)	(b) (4)
60	TT GE Kiosks Misc. Svcs	1.000	AU	(b) (4)	(b) (4)
60 cont.	Freight, various misc. hardware; site prep/cabling; printing paper; travel				
70	TT Labor	1.000	AU	(b) (4)	(b) (4)
80	TT Labor	1.000	AU	(b) (4)	(b) (4)
90	TT Labor	1.000	AU	(b) (4)	(b) (4)
100	GE Kiosk Systems	38.000	EA	(b) (4)	(b) (4)
100 cont.	KIS CBP Global Entry 10-Print, Dual-Printer Style Kiosk System;  19 each @ (b) (4)  Contains CPU High risk sensitive.				
110	KIS CBP Global Entry one year factory wa	1.000	AU	(b) (4)	(b) (4)
120	Acapela Heather Voice Multimedia	38.000	EA	(b) (4)	(b) (4)
130	Aware Runtime License and Annual Maint	38.000	EA	(b) (4)	(b) (4)
140	TT Labor	1.000	AU	(b) (4)	(b) (4)
150	Misc ODCs/Services	1.000	AU	(b) (4)	(b) (4)
160	Misc SW/Maint	1.000	AU	(b) (4)	(b) (4)
170	Dell 760 Optiplex	1.000	EA	(b) (4)	(b) (4)
180	Travel	1.000	AU	(b) (4)	(b) (4)
190	Misc Equipment	1.000	EA	(b) (4)	(b) (4)
200	PALS Server	1.000	EA	(b) (4)	(b) (4)
210	InstallShield 2011 Pro + Maint	1.000	EA	(b) (4)	(b) (4)
220	Guardian Edge Encryption SW	4000.000	EA	(b) (4)	(b) (4)
230	Guardian Edge Encryption SW for PALS Lap	2000.000	EA	(b) (4)	(b) (4)
240	Toughbook CF-52ELNHQ2M	14.000	EA	(b) (4)	(b) (4)
240 cont.	LPT-0614 POC (b) (6) - (b) (6)  Resolution must be no less than 1280 x 1024 Vista COA Intel Core 2 Duo P8600 2.4 GHz (Centrino2 vPRO) AMT 160 GB Hard drive (shock-mounted and quick-release) 2GB 512 MB VRAM Win SP Intel Wireless Wifi Link 5100 8.2.11a/b/g/n				

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
	Multi-drive Bluetooth Gobi mobile broadband (WWAN) SmartCard Fingerprint Battery Charging: 4hrs CPU w/touchscreen: 8hrs. (w/long life battery) Weight varies by battery type: 7.2 or 7.5 lbs. (without touchscreen) 7.6 or 7.9 lbs. (with touchscreen) Display Options: Intel P8600: 15.4" WUXGA ATI Radeon HD 3650 dedicated VRAM Intel P8400: 15.4" WXGA AG & AR (AR only on P8600 & P8400 w/touchscreen)				

Total Funded Value of Award:

\$9,999,818.93

**I.2 ACCOUNTING and APPROPRIATION DATA**

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2525USCSGLCS0923050000Z63F10400AP01 640602525	(b) (4)
20	6100.2525USCSGLCS0923050000Z63F10400AP01 640502525	(b) (4)
30	6100.2525USCSGLCS0923050000Z63F10400AP01 640902525	(b) (4)
40	6100.2525USCSGLCS0923050000Z63F10400AP01 IS4502525	(b) (4)
50	6100.2525USCSGLCS0923050000Z63F10400HQ01 IS4302525	(b) (4)
60	6100.2525USCSGLCS0923050000Z63F10400AP11 IU4702525	(b) (4)
70	6100.2525USCSGLCS0923050000Z63F10400AP11 IU4702525	(b) (4)
80	6100.2525USCSGLCS0923050000Z63F10400AP11 IU4702525	(b) (4)
90	6100.2525USCSGLCS0923050000Z63F10400AP11 IU4702525	(b) (4)
100	6100.316AUSCSGLCS0923050000Z63F10400AP11 IU470316A	(b) (4)
110	6100.2574USCSGLCS0923050000Z63F10400AP11 IU4702574	(b) (4)
120	6100.315AUSCSGLCS0923050000Z63F10400AP11 IU470315A	(b) (4)
130	6100.315AUSCSGLCS0923050000Z63F10400AP11 IU470315A	(b) (4)
140	6100.2525USCSGLCS0923050000Z63F10400AP05 IU4702525	(b) (4)
150	6100.2525USCSGLCS0923050000Z63F10400AP01 640602525	(b) (4)
160	6100.2574USCSGLCS0923050000Z00010400AP01 640602574	(b) (4)
170	6100.316AUSCSGLCS0923050000Z63F10400AP01 64060316A	(b) (4)
180	6100.2525USCSGLCS0923050000Z63F10400AP01 640602525	(b) (4)
190	6100.319BUSCSGLCS0923050000Z63F10400AP01 64060319B	(b) (4)
200	6100.316AUSCSGLCS0923050000Z63F10400AP01 64060316A	(b) (4)
210	6100.315AUSCSGLCS0923050000Z63F10400AP01 64060315A	(b) (4)
220	6100.315AUSCSGLCS0923050000Z63F10400AP01 64060315A	(b) (4)
230	6100.315AUSCSGLCS0923050000Z63F10400AP01 64060315A	(b) (4)
240	6100.316AUSCSGLCS0923050000Z63F10400AP01 64060316A	(b) (4)

**I.3 DELIVERY SCHEDULE**

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 7400 Fullerton Road Springfield, VA 22153	10	1.000	02/01/2011
	20	1.000	02/01/2011
	30	1.000	02/01/2011
	40	1.000	02/01/2011
	50	1.000	02/01/2011

<b>DELIVER TO:</b>	<b>ITEM #</b>	<b>QTY</b>	<b>DELIVERY DATE</b>
	60	1.000	02/01/2011
	70	1.000	02/01/2011
	80	1.000	02/01/2011
	90	1.000	02/01/2011
	100	38.000	02/01/2011
	110	1.000	02/01/2011
	120	38.000	02/01/2011
	130	38.000	02/01/2011
	140	1.000	02/01/2011
	150	1.000	02/01/2011
	160	1.000	02/01/2011
	170	1.000	02/01/2011
	180	1.000	02/01/2011
	190	1.000	02/01/2011
	200	1.000	02/01/2011
	210	1.000	02/01/2011
	220	4000.000	02/01/2011
	230	2000.000	02/01/2011
	240	14.000	02/01/2011

**I.4 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.5 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.6 NON-PERSONAL SERVICE (MAR 2003)**

1. The Government and the contractor agree and understand the services to be performed under this contract are non-personal in nature. The Contractor shall not perform any inherently Governmental functions under this contract as described in Office of Federal Procurement Policy Letter 92-1

2. The services to be performed under this contract do not require the Contractor or his employees to exercise personal judgment and discretion on behalf of the Government, but rather, the Contractor's employees will act and exercise personal judgment and discretion on behalf of the Contractor.
3. The parties also recognize and agree that no employer-employee relationship exists or will exist between the Government and the Contractor. The Contractor and the Contractor's employees are not employees of the Federal Government and are not eligible for entitlement and benefits given federal employees. Contractor personnel under this contract shall not:
  - (a) Be placed in a position where there is an appearance that they are employed by the Government or are under the supervision, direction, or evaluation of any Government employee. All individual employee assignments any daily work direction shall be given by the applicable employee supervisor.
  - (b) Hold him or herself out to be a Government employee, agent or representative or state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as such and specify the name of the company of which they work.
  - (c) Be placed in a position of command, supervision, administration or control over Government personnel or personnel of other Government contractors, or become a part of the government organization. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to change the contract in any way. If the other Contractor believes this communication to be direction to change their contract, they should notify the CO for that contract and not carry out the direction until a clarification has been issued by the CO.
4. If the Contractor believes any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, the Contractor shall promptly notify the CO of this communication or action.
5. Rules, regulations directives and requirements which are issued by U.S. Customs & Border Protection under their responsibility for good order, administration and security are applicable to all personnel who enter U.S. Customs & Border Protection installations or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract.

[End of Clause]

## **I.7 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.8 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]



**HSAR Clauses to be include in the Contract**

**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 10 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.

(End of clause)

**3052.204-71 Contractor employee access.**

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

**CONTRACTOR EMPLOYEE ACCESS(JUN 2006)**

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

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

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

(End of clause)

**ALTERNATE I  
(JUN 2006)**

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

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

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

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

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

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

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

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

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

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

(End of clause)

## 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 Tool (DART)**

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

## DHS CLAUSES

use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

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

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

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

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

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

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

### **Section 508 Applicable Exceptions**

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

### **Section 508 Compliance Requirements**

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in

## DHS CLAUSES

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

### 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.

- **System Security documentation appropriate for the SDLC 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

## DHS CLAUSES

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

## DHS CLAUSES

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.

### Engineering Platforms

- **Common Enterprise Services (CES)** – Deliver the systems, infrastructure, and operational capabilities to fully implement the three service levels defined as part of the DHS/CBP Common Enterprise Services and support DHS Component use of those services. This includes the build out and integration of all required services and infrastructure, which must include the Single Sign-on Portal and CBP Enterprise Services Bus (ESB), required for the CES. Capabilities shall be designed to the DHS standard operating architecture (SOA), transportable between DHS data centers (CBP National Data Center, Stennis, and DHS 2<sup>nd</sup> data center).
- **Single Sign-on Portal** – Design, build, and operate a single sign-on Portal - consistent with DHS' enterprise portal solution (for which ICE is the steward) - to provide a common point of access, with a single sign-on capability to existing applications and to provide the infrastructure for integrating diverse internal and/or external information and transactional resources. This includes the migration of the current ACE Portal to the Single Sign-on Portal as rapidly as feasible.

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

## DHS CLAUSES

- **PROVIDE EXPLANATION: Software is already in production and will migrate to Stennis**
- **Help Desk and Operations Support**

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

- **Interfacing**

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

### **TRANSITION PLAN (if applicable)**

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

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

### **Portfolio Review**

**To what primary DHS IT Portfolio does this acquisition request align?**

**Screening/Watchlist/Credentialing**

**DHS CLAUSES**

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