AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE	PAGE 1 OF PAGES 2

2. AMENDMENT/MODIFICATION NO.	3. EFF. DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
P00009	07/07/2010	0020027393	

6. ISSUED BY CODE 70050800
DHS - Customs & Border Protection
DHS, Customs & Border Protection
6650 Telecom Dr. Intech Two St
ATTN: (b) (6) [redacted]
Indianapolis IN 46278

7. ADMINISTERED BY (If other than Item 6) CODE
DHS - Customs & Border Protection
DHS, Customs & Border Protection
6650 Telecom Dr. Intech Two St
ATTN: (b) (6) [redacted]
Indianapolis IN 46278

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and Zip Code)
KFORCE GOVERNMENT SOLUTIONS INC

2750 PROSPERITY AVE (STE 300)
STE 300
FAIRFAX VA 22031-4312

CODE 072650484 FACILITY CODE

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED (SEE ITEM 11)

10A. MODIFICATION OF CONTRACT/ORDER NO. / HSBP1007J17675

10B. DATED (SEE ITEM 13) 07/25/2008

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)

see attached

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 data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103 (b).

☒ C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 43-103(A)3

D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not ☒ is required to sign this document and return 1 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 bilateral modification is to deobligate funds, incorporate revised Statement of Work, and Exercise Option Year 3 of Task Order HSBP1007J1765 for Audit Support Service

1. Deobligate funds from line 0010 changing the amount from (b) (4) [redacted] to read (b) (4) [redacted]; a decrease of (b) (4) [redacted].
2. Deobligate funds from line 0020 changing the amount from (b) (4) [redacted] to read (b) (4) [redacted]; a decrease of (b) (4) [redacted].
3. The total amount of deobligations is $205,064.63.
4. Total obligated amount of this Task Order is changed from $6,701,777.32 to read $6,496,712.69; a decrease of $205,064.63.

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)	
(b) (6) [redacted], Vice President FMAS		Bruce D. Wood	
15B. CONTRACTOR/OFFEROR (b) (6) [redacted] (Signature of person authorized to sign)	15C. DATE SIGNED 7/15/2010	(b) (6) [redacted]	16C. DATE SIGNED 7/16/10

NSN 7540-01-152-8070
PREVIOUS EDITION UNUSABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA FAR (48 CFR) 53.243

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

5. Incorporate the attached revised Statement of Work entitled, "Statement of Work – Exercise of Option Year 3.

6. Option Year 3 is hereby exercised. Performance Period is changed from 7/25/2009 – 7/24/2010 to read 7/25/2010 – 7/24/2011 an increase of 365 calendar days.

7. Add line item 170 to increase Task Oder in the amount of (b) (4) [redacted].

8. Add line item 180 to increase the Task Order in the amount of (b) (4) [redacted].

9. Add line item 190 to increase the Task Order in the amount of (b) (4) [redacted].

10. Add line item 200 to increase the Task Order in the amount of (b) (4) [redacted].

11. The total amount obligated for Option Year 3 is $1,656,605.68.

12. The total obligated amount of this Task Order is changed from $6,496,712.69 to read $8,153,318.37, an increase of $1,656,605.08.

13. All other terms and conditions under this Task Order remain unchanged.

ATTACHMENT INFORMATION
FOR
AWARD/ORDER/IA MODIFICATION: HSBP1007J17675P00009

I.1 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	Base Period Contract Audit Liaison-Labor	1.000	AU	(b) (4)	
20	Contract Audit Liaison	1.000	AU		
30	Contract Audit Liaison	1.000	AU		
40	Base Period Contract Audit Liaison-Labor	1.000	AU		
60	Audit Support - EDME	1.000	AU		
70	ACE support - KForce	1.000	AU		
80	ENTS Audit Liaison Support	1.000	AU		
90	Travel	1.000	AU		
100	Audit Support - EDME	1.000	AU		
110	EDME Audit and QA Support	1.000	AU		
120	EDME Audit and QA Support	1.000	AU		
130	PCB Audit Support	1.000	AU		
140	ETP Audit & Quality Assurance	1.000	AU		
150	Travel for EDME	1.000	AU		
160	ETP Audit & Quality Assurance	1.000	AU		
170	EDME Audit Support	1.000	AU		
180	ETP Audit & Quality Assurance	1.000	AU		
190	ETP Audit & QA Travel	1.000	AU		
200	EDME Audit Travel	1.000	AU		

Total Funded Value of Award: **$8,153,318.37**

I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2525USCSGLCS0923020000Z00007164HQ01 IR1042525	(b) (4)
20	6100.2525USCSGLCS0923030300Z00007164HQ01 IR2302525	
30	6100.2525USCSGLCS0923030300Z00007165HQ01 IS6062525	
40	6100.2525USCSGLCS0923030000Z00007400HQ01 IR2012525	
60	6100.2525USCSGLCS0923030000Z00008400BN01 IR2012525	
70	6100.2525USCSGLCS0923030000Z00008165HQ01 IS6062525	
80	6100.2525USCSGLCS0923020000Z00008400AP06 IR1012525	
90	6100.2525USCSGLCS0923030000Z00008400BN01 IR2012525	
100	6100.2525USCSGLCS0923030000Z00008400HQ01 IR2012525	
110	6100.2525USCSGLCS0923030000Z00009400HQ01 IR2332525	
120	6100.2525USCSGLCS0923030000Z00009165HQ01 IS6442525	
130	6100.2525USCSGLCS0923030000Z65A10400HQ01 IR2312525	
140	6100.2525USCSGLCS0923020400Z65A10400HQ01 IR1802525	
150	6100.2525USCSGLCS0923030000Z65A10400HQ01 IR2312525	
160	6100.2525USCSGLCS0923020400Z65A09173SB02 IU1802525	
170	6100.2525USCSGLCS0923030000Z65A10400HQ01 IR2332525	
180	6100.2525USCSGLCS0923020400Z65A09173SB02 IU1802525	
190	6100.2525USCSGLCS0923020400Z65A09173SB02 IU1802525	
200	6100.2525USCSGLCS0923030000Z65A10400HQ01 IR2332525	

I.3 DELIVERY SCHEDULE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 7681 Boston Blvd Springfield, VA 22153	10	1.000	06/05/2007
	20	1.000	05/31/2007
	30	1.000	05/31/2007
	40	1.000	09/06/2007
	60	1.000	07/27/2008
	80	1.000	04/09/2008
	100	1.000	07/27/2008
	110	1.000	07/24/2010
	120	1.000	07/24/2010
	130	1.000	11/30/2009
	140	1.000	03/02/2010
	150	1.000	02/28/2010
	160	1.000	03/02/2010
	180	1.000	07/24/2011
	190	1.000	07/24/2011
Customs and Border Protection 7715-F Fullerton Road Springfield, VA 20598	70	1.000	04/01/2008
	90	1.000	07/16/2008
	170	1.000	10/01/2009
	200	1.000	07/24/2011

Statement of Work (SOW)–Exercise of Option Year 3

(Option 3 Period of Performance 7/25/10 through 7/24/11)

1. **PROJECT TITLE:** CBP Office of Information and Technology Audit Liaison Support and Quality Assurance Services

2. **BACKGROUND:** The Office of Information and Technology (OIT), Bureau of Customs and Border Protection (CBP) mission is to enforce the laws of more than 40 agencies and to protect the revenue of the United States while facilitating trade. OIT is responsible for the operation and maintenance of the information technology systems required to support DHS and CBP missions. In this role, OIT is subject to oversight by the General Accountability Office (GAO) and the Department of Homeland Security Office of the Inspector General (OIG); the Office of Management and Budget. In the past fiscal year OIT was involved in over 59 external audits and reviews. By law, OIT is mandated to respond promptly, completely, and accurately to OIG or GAO initiated audits. OIT is seeking ongoing audit liaison support services and quality assurance services to ensure the timeliness, accuracy and efficiency in responding to the Auditor request demands and to be proactive in executing a quality management program.

3. **SCOPE:**

   3.1 The Contractor shall work collaboratively with the Chief, Audit Liaison for the Office of Information Technology in coordinating external assessments and in monitoring progress of Corrective Action Plans to remedy weaknesses identified during external assessments.

   3.2 The Contractor shall also work collaboratively with OIT Program Office or Division Task Monitors for the Office of Information Technology in conducting internal quality assurance assessments and in monitoring progress of Corrective Action Plans to remedy weaknesses identified during internal assessments.

4. **APPLICABLE DOCUMENTS:**

   - DHS Management Directive 077-02 Relations with the U.S. Government Accountability Office
   - DHS Management Directive 0810.1 The Office of Inspector General
   - DHS Reference Pamphlet "Safeguarding Classified & Sensitive Unclassified Information"
   - Inspector General Act of 1978 as amended, 5 U.S.C. app. (2000)
   - Chief Financial Officers act of 1990 (Public Law 101-156)
   - Government Management Report Act of 1994 (Public Law 103-356)
   - Office of Management and Budget (OMB) Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations
   - Policy for OIT Plan of Actions and Milestones (POAM) Process, OIT QM 2.03
   - Policy for Responding to External Audits, OIT QM 2.05

5. SPECIFIC TASKS:

5.1 Task 1 - Audit Liaison/Coordination Support

The Contractor shall assist in the coordination of external assessments (audits, reviews and surveys) by the General Accounting Office, the DHS Office of the Inspector General and other oversight organizations. The Contractor shall also assist in evaluating the results from external assessments (findings and recommendations), developing corrective action plans and monitoring progress on corrective action plans of the OIT operations for CBP. Specific tasks include:

5.1.1 Interacting effectively with personnel across OIT, within other CBP offices, and with external audit organizations to ensure that ongoing audits progress smoothly and to facilitate the timely resolution of outstanding audit issues.

5.1.2 Maintaining the web based audit and reviews tracking database and develop reports and queries to help present the status of audit information in an easily readable format for management review.

5.1.3 Analyzing findings and recommendations identified during audits and reviews to ensure accuracy and validity and assurance that they translate into actionable plans to resolve identified weaknesses.

5.1.4 Facilitating development of corrective action plans by CBP personnel and assess whether proposed actions or completed actions adequately address recommendations.

5.1.5 Reviewing supporting documentation to ensure it is adequate to support recommendations.

5.1.6 Researching audit and risk management issues to develop proposals to improve OIT's internal control environment.

5.2 Task 2 - Quality Assurance Services

The purpose of this task is to provide ongoing support in executing OIT's Division/Program Office Quality Management Program on an as needed basis. The Contractor shall assist in the coordination of internal assessments (audits, reviews and surveys). The Contractor shall also assist OIT personnel and management in evaluating the results from internal assessments, assist OIT staff in developing corrective action plans and monitoring progress on corrective action plans of the OIT operations for CBP. OIT Divisions or Program Offices will establish separate task orders for Quality Assurance Services. The Contractor shall participate in the OIT QA activities, as directed by the Contracting Officer's Technical Representative (COTR) or Task Monitor. Specific tasks may include:

- Defining quality goals and measures
- Developing and maintaining: a QA Plan, QA Metrics Plan, QA Processes and Procedures, QA templates, and QA Audit Criteria for QA Processes and Procedures
- Developing and maintaining a QA Internal Audit Schedule
- Scheduling, preparing and executing QA audits as needed within the Office of Information and Technology. These audits are to include, but are not limited to, division/branch/project level audits, pre-stage exit audits, and OIT level audits
- Assisting in post audit follow-up activities to ensure that audit findings (on both internal and external reviews and assessments) are addressed
- Participating in any outside audits (e.g. GAO, IG, OMB, etc.) conducted on OIT
- Assisting in the review of the OIT's QA function on a periodic basis to monitor the effectiveness of the QA Program by coordinating and participating in independent quality audits
- Developing and maintaining data in review and assessment tracking and control tools (which includes data and meeting requests, action items, plan of actions and milestones, risks, findings, trends, etc.)

6. DELIVERABLES AND DELIVERY SCHEDULE:

6.1 Task 1

Deliverable Title & Delivery Date: Weekly Activity Report to address work completed during the current period, planned activities for the next period and any related problems or issues. Report is to be submitted to the COTR as one soft copy via email no later than 12:00 P.M. each Thursday.

6.2 Task 2

Deliverable Title: At the onset of each new QA Task; the Task Monitor will define specific deliverables and due dates. The Contractor shall prepare QA reports and briefings, prepare and conduct QA training, and prepare newsletters, articles, and other forms of QA communications, as directed by Division/Program Office Task Monitors. Deliverables and Schedules, for new QA tasks may include, but are not limited to the following:

- Maintenance of OIT QA processes/procedures for the following: OIT QA Plan, OIT QA Metric Plan, OIT CM Plan QA Section and OIT QA templates
- Production of QA Reports
- Production of QA Training and Briefings
- Proposed Newsletter articles and other forms of communication
- Participation in Process Improvement activities and assessments
- Participation in Process Improvement and OIT QA activities Update/change and documentation of QA Databases Maintenance of QA Audit Schedule and QA Internal Schedule

- Maintenance of the QA Process Action Library (PAL) (to include the Corrective Action Database) Prepare and Conduct QA Audits to include metric collection, trend analysis, and follow-up

6.3 Quality Measures

The general quality measures as set forth below will be applied to each Work Product received from the Contractor under this Task Order.

6.3.1 **Accuracy** – Work Products shall be accurate in presentation, technical content, and adherence to accepted elements of style.

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

6.3.3 **Specifications Validity** – All Work Products must satisfy the requirements of the Government as specified herein.

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

6.3.5 **Timeliness** – Work Products shall be submitted on or before the due date specified in this Purchase Order or other negotiated delivery schedule.

7. GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION:

7.1 Government-Furnished Equipment

The Government will provide, for all contractor Government-site personnel, on-site facilities to perform any work required under this task order. The Government-site facilities will consist of a desk, chair, telephone, computer equipment with LAN/WAN interface, document file cabinets, access to copiers and fax machines and consumable supplies for personnel working directly on this contract. All work shall occur on government provided equipment. The Contractor will be provided access to Government information as needed in the performance of the task.

7.2 Government Furnished Information

- OMB Circular A-11
- DHS Management Directive 1400 (Currently in draft. Latest version will be provided.)
- CBP Pre-Select Process Document (Currently in draft, awaiting approval)
- U.S. CBP Security Policies and Procedures Handbook CIS HB 1400-05B

- DHS Life-Cycle CPIC Guidance

The above documents are basic to the Investment Management Process (IMP) at CBP. The Contractor may require other documents during the course of work with various projects. Such documentation will be provided as needed, and may include, but are not limited to, such documents as:

- DHS Guidance on the Privacy Impact Assessment
- DHS Mission Needs Statement template and instructions
- DHS Program Management Plan
- DHS Management Directive 1330 Planning, Programming, Budget and Execution
- FEA Reference Models
- CBP Systems Development Life Cycle Handbook
- Customs Directive No. 51715-006 Separation Procedures for Contractor Employees (CF-242)

8. PLACE OF PERFORMANCE:

The Contractor will be allowed limited access to the Government's facilities, as specified below:

Customs and Border Protection (Bostons)
7375 Boston Boulevard
Springfield, VA 22153

Customs and Border Protection National Data Center (NDC4 & 5)
7451 and 7435 Boston Boulevard
Springfield, VA 22153

Customs and Border Protection National Data Center (NDC3)
7400 Fullerton Road
Springfield, VA 22153

Customs and Border Protection National Data Center (NDC2)
7501 Boston Boulevard
Springfield, VA 22153

Customs and Border Protection (Beauregard)
1801 N Beauregard Street
Alexandria, VA 22311

Customs and Border Protection National Data Center (NDC1)
7681 Boston Boulevard
Springfield, VA 22153

Customs and Border Protection Headquarters (RRB)
1300 Pennsylvania Ave., NW

Washington, D.C. 20229

Customs and Border Protection (Kingstowne)
597 Kingstowne Village Dr.
Alexandria, VA 22315

Customs and Border Protection (Tysons)
8020 Towers Crescent Dr
Vienna, VA 22182

Customs and Border Protection (Falls Church)
7799 Leesburg Pike
Falls Church, VA 22043

9. DUTY HOURS:

9.1 The Contractor shall provide support, as directed, during core working hours (8: 30 AM – 5:00 PM), Monday through Friday, excluding Government holidays. Full time employees working on this task order shall work a 40-hour workweek, with a standard workday consisting of an eight hour workday plus a half hour (non-compensated) lunch break. The contract staff shall start no earlier than 7:00 AM, leave no earlier than 4 PM, nor work later than 6:00 PM. Deviations to the standard schedule, must be submitted in writing by the Contractor's Project Manager for approval. The COTR or assigned Task Monitors, at their discretion may approve alternate work schedules. The Contractor's Program Manager shall verify with the COTR the standard work schedules for the contract staff and any changes to the schedules.

9.2 Assigned Task Monitors (TM's) will have the authority (delegated by the COTR) to approve requests for deviations from the defined work schedule (to include overtime hours billed as noted below). Requests for deviations from the defined work schedule must be submitted for prior approval in writing (e-mail preferred) by the contractor's team member to their TM. TM's will provide e-mail notification of approved requests to the COTR and contractor's Project Manager. Urgent, verbal requests and approvals must be subsequently documented in writing. Billing rates for overtime work will be the same as the standard billing rate for the individual under this contract. (However, for individuals classified as non-exempt under the Fair Labor Standards Act, billing rates for hours worked in excess of 40 hours a week will be one-and-a-half times the standard billing rate for the individual under this contract).

10. INVOICING:

The contractor shall submit invoices electronically to the COTR and to the following:

US Customs and Border Protection
National Finance Center
P.O. Box 68908
Indianapolis., IN 46268
cbpinvoices@dhs.gov

EDME Budget
edmebudget@cbp.dhs.gov

11. TRAVEL:

In accordance with the Federal Travel Regulation (FTR), travel costs not to exceed (b) (4) per year may be required for this effort. While the majority of travel is expected to be within the local Washington DC Metro Area on occasion a contractor may be asked to travel nationally to any CBP field sites.

12. TRANSITION PLANNING:

End of Task Order: Initial transition planning may be required at the time of this contract's expiration. The successful Contractor under this contract will be required to agree to:

- Furnish phase-in training
- Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor
- Furnish phase-in, phase-out services for up to 30 days after the task order expires
- Negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required
- Allow as many current personnel as practicable to help the continuity and consistency of the services required by this contract
- Disclose the necessary personnel records to allow the successor to conduct on-site interviews with their employees
- If selected employees are agreeable to change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor

13. **ESTIMATED LEVEL OF EFFORT:** Government Labor Categories and estimated hours:

Tasks 1 and 2 Combined - Audit Liaison and Quality Assurance Task Order
Base Period and Option Years

		Not To Exceed "X" Number of Hours				
Labor Categories	Number of Personnel	Base Period	Option Yr 1	Option Yr 2 through 4 Personnel	Option Yr 2	Optional Yr 3 and 4 Personnel
(b) (4)						
	TOTAL	(b) (4)				

Tasks 1 and 2 Combined- Audit Liaison and Quality Assurance Task Order
Optionals

		Not To Exceed "X" Number of Hours				
Labor Categories	Number of Personnel	Base Period Optional	Optional Yr 1	Optional Yr 2 through 4 Personnel	Option Yr 2	Optional Yr 3 and 4 Personnel
(b) (4)						
	TOTAL	(b) (4)				

Task 1 - Audit Liaison/Coordination Task Order
Base Period and Option Years

Labor Categories	Number of Personnel	Base Period	Option Yr 1	Option Yr 2 through 4 Personnel (no change from base)	Option Yr 2	Optional Yr 3 and 4 Personnel
(b) (4)						
TOTAL	(b) (4)					

Task 1 Audit Liaison/Coordination Task Order
Optionals

		Not To Exceed "X" Number of Hours				
Labor Categories	Number of Personnel	Base Period Optional	Optional Yr 1	Optional Yr 2 through 4 Personnel	Option Yr 2	Optional Yr 3 and 4 Personnel
(b) (4)						
TOTAL	(b) (4)					

Task 2- Quality Assurance Task Order
Base Period and Option Years

		Not To Exceed "X" Number of Hours				
Labor Categories	Number of Personnel	Base Period	Option Yr 1	Option Yr 2 through 4 Personnel	Option Yr 2	Optional Yr 3 and 4 Personnel
(b) (4)						
TOTAL	(b) (4)					

Task 2- Quality Assurance Task Order
Optionals

		Not To Exceed "X" Number of Hours				
Labor Categories	Number of Personnel	Base Period Optional	Optional Yr 1	Optional Yr 2 through 4 Personnel	Option Yr 2	Optional Yr 3 and 4 Personnel
(b) (4)						

14. PERIOD OF PERFORMANCE:

This task order will consist of a base period and four (4) one year option periods. The base period of performance for this task order ran from September 24, 2007 through July 24, 2008. Each option year shall run for twelve months thereafter, beginning July, 25th 2008 as follows:

Task Order Period	Start	End
Base Period	9/24/07	7/24/2008
Option Period 1	7/25/2008	7/24/2009
Option Period 2	7/25/2009	7/24/2010
Option Period 3	7/25/2010	7/24/2011
Option Period 4	7/25/2011	7/24/2012

15. SECURITY:

The Contractor shall comply with the Customs administrative, physical and technical security controls to ensure that the Government's security requirements are met. During the course of this Task Order, the Contractor shall not use, disclose, or reproduce data, which bears a restrictive legend, other than as required in the performance of this Order.

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. 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.

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*

15.1 Personnel Security Background Data

15.1.1 All personnel employed by the contractor or responsible to the contractor for work performed hereunder shall either currently possess or be able to favorably pass a full-field five (5) year background investigation (BI) required by CBP policies and procedures for employment prior to beginning work with CBP. This policy applies to any new personnel hired as replacement(s) during the term of this contract. Due to CBPs Mission and the ever changing Information and Technology security environment there may be a future requirement that all contract personnel obtain additional security clearances. Clearance levels may range from Secret up through Top Secret. COTR will notify the contractor of this requirement and will provide details as to which personnel need to obtain them, the level clearance required and the time frame for obtaining them. The cost shall be borne by the contractor.

15.1.2 Prior to bringing new hires on site, the contractor shall submit the full name, social security number, and date of birth of the individual who will require a background investigation by CBP, and submit such information and documentation as may be required by the Government to have a BI performed.

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

15.1.4 All background investigation forms must be accepted by CBP with verbal approval from a representative of the CBP Office of Management Inspection and Integrity Assurance, Security Program Division (MIIA-SPD) before contract personnel can begin work under this order. MIAA-SPD estimates these procedures will take approximately ten (10) days from the time they receive the packet. Currently, completion of background investigations is taking approximately six (6) months from initial acceptance of the package.

15.1.5 The contractor shall notify the COTR and CBP Office of Information and Technology (OIT) Workforce Management Group (WMG), BI Coordinator of any changes in access requirements for its personnel no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and reassignments including those to another contract. The Contractor/Project Manager is responsible for the completion and timely submission to the COTR of the CF-242 for all departing contract personnel. The Contractor shall provide OIT/WMG/BI Coordinator the following information on behalf of their contract personnel to telephone number 703-921-6237 or fax the below information to 703-921-6780:

FULL NAME
SOCIAL SECURITY NUMBER
EFFECTIVE DATE
REASON FOR CHANGE

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

15.2 Identification Badges

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

15.3 Additional Personnel Security Data

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

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

15.4 Contractor Employee Access

15.4.1 Sensitive Information – Sensitive information, as used in this Section, 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:

15.4.1.1 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);

15.4.1.2 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);

15.4.1.3 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

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

15.4.1.5 "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.

15.4.1.6 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 subjected 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.

15.4.1.7 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.

15.4.1.8 Work under this task order 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.

15.4.1.9 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.

15.4.1.10 Before receiving access to IT resources under this contract the individual must receive a security briefing, which the COTR will arrange, and complete any non-disclosure agreement furnished by DHS.

15.4.1.11 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.

15.4.1.12 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).

15.4.1.13 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.

15.4.1.14 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.

15.5 Security Requirements For Unclassified Information Technology Resources

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.

15.5.1 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.

15.5.2 Within 30 days after task order renewal, the contractor shall submit for approval its IT Security Plan. 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. The security plan shall specifically include instructions regarding handling and protecting sensitive information on and offsite (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.

15.5.3 Examples of tasks that require security provisions include:

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

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

15.5.4 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.

15.6 Monitoring/reviewing contractor security requirements clause

15.6.1 Security Review and Reporting

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.

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

16. ACCESSIBILITY REQUIREMENTS (SECTION 508 COMPLIANCE):

16.1 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.

16.2 All Electronic and Information Technology (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:

16.2.1 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.

16.2.2 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.

16.2.3 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.

16.3 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:

16.3.1 36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards.

16.4 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.

16.4.1 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.

17. ENTERPRISE ARCHITECTURE (EA) COMPLIANCE CLAUSES:

Compliance with the Homeland Security (HLS) EA shall be derived from and aligned through the CBP EA.

17.1 HLS EA Clause – Design Conformance to DHS/CBP EA, TRM, Policy:

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.

17.2 HLS EA Clause – Development Solutions Conformance to FEA Standards:

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.

17.3 HLS EA Clause – Development, Testing, and Implementation Solutions Conformance to DHS/CBP TRM Standards:

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.

17.4 HLS EA Clause – Developed Solutions:

All developed solutions shall be compliant with the HLS EA.
All developed solutions shall be compliant with the system life cycle and use of Worklenz for reporting purposes.

17.5 HLS EA Clause – Hardware/Software:

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

17.6 HLS EA Compliance for Data:

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.

17.7 IPv6 Clauses

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.

All Information Technology assets being developed, procured, or acquired shall be IPv6 capable.

18. ENGINEERING PLATFORMS:

18.1 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).

18.2 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.

19. INFRASTRUCTURE TRANSFORMATION PROGRAM (ITP) COMPLIANCE AND ITP TRANSITION PLAN:

The services under this Task Order are not being relocated to Stennis. As such, the clauses under this section have been omitted from the SOW as they are not applicable.

20. PORTFOLIO REVIEW:

Data Management – Includes all Information Management activities, including coordinating information collection, storage, dissemination, and destruction. This also includes managing information management policies, guidelines, and standards.

21. NON-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 SOW. The information shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this order on an Official Use Only or need to know basis.

Upon award, the contractor shall provide to the COTR a signed DHS 11000-6 Standard Non-Disclosure Agreement Form for each employee working under the contract. The contractor shall also provide this signed form each time a new employee is assigned to the contract.