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

2. AMENDMENT/MODIFICATION NO.	3. EFF. DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
P00001	07/23/2010	0020051154	

6. ISSUED BY CODE 70050800

DEPARTMENT OF HOMELAND SECURITY
U.S. CUSTOMS AND BORDER PROTECTION
1300 PENNSYLVANIA AVENUE, N.W.,
SUITE NP-1310
WASHINGTON DC 20229

7. ADMINISTERED BY *(If other than Item 6)* CODE

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State and Zip Code)*

IBM CORP

1755 JEFFERSON DAVIS HWY
SUITE 504
ARLINGTON VA 22202

CODE 000000000 FACILITY CODE

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED *(SEE ITEM 11)*

☒ 10A. MODIFICATION OF CONTRACT/ORDER NO. / HSBP1010F00171

10B. DATED *(SEE ITEM 13)* 07/01/2010

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

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

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

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

☒ A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

☐ B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(Such as changes in paying office, appropriation date, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103 (b).

☐ C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

☐ D. OTHER *(Specify type of modification and authority)*

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

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

THIS MODIFICATION P00001 TO DELIVERY ORDER HSBP1010F00171 INCORPORATES THE ATTACHED REVISED STATEMENT OF WORK DATED JUNE 23, 2010, AND INCREASES THE OBLIGATED AMOUNT OF THE ORDER BY $936,860.00 FROM $3,488,795.00 TO $4,425,655.00.

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)*	
		MICHAEL REBAIN CONTRACTING OFFICER	
15B. CONTRACTOR/OFFEROR *(Signature of person authorized to sign)*	15C. DATE SIGNED	16B. BY (b) (6) [redacted]	16C. DATE SIGNED 07/23/2010

Department of Homeland Security
U.S. Customs and Border Protection, Office of Administration
Financial Systems Division

Statement of Work - Revised
For
Development/Support Service for SAP Project

July 23, 2010

1.0 BACKGROUND

The U.S. Customs and Border Protection (CBP), Office of Administration (OA), Financial Systems Division (FSD) has identified an ongoing requirement for integration support services for implementing, operating and maintaining the OF-SAP System. The effort includes support related to the development of SAP integration/interfaces to new systems (for example, the current FedTraveler project. The specific requirement represented by this action will be in support of the defined scope for the Legacy Customs Release 3 implementation and ongoing post production support for the CBP Releases 1, 2, and 3 SAP R/3 and Enterprise (ECC) platforms.

2.0 SCOPE OF WORK

The scope of work for this requirement is the execution of the Project Charters for Releases 1, 2, 3, and Post Production, as well as the requirements estimating model and staffing plan for the SAP Project as defined by CBP (most recently Post Production during FY10).

3.0 PERIOD OF PERFORMANCE

The period of performance for this requirement is the period June 30, 2010, through October 31, 2010.

4.0 PLACE OF PERFORMANCE

Work under this task order may be performed in multiple locations to include Indianapolis, IN and Washington, DC.

5.0 INFORMATION TECHNOLOGY COMPLIANCY AND STANDARDS

Work under this task order must comply with all applicable information technology compliancy and standards, as detailed in Attachment A.

All encryption shall be FIPS 197 Advanced Encryption Standard (AES) that has been FIPS 140-2 certified.

6.0 DESCRIPTION OF TASKS AND DELIVERABLES

6.0.1 All work under this SOW will be performed in accordance with the contractor's GSA Schedule Contract GS-35F-4984H. The Contractor will follow the same project management and team based approach to completing the work as has been employed during all previous tasks supporting the SAP Project.

The Contractor will assist CBP personnel with the following tasks:

- Operations & maintenance for the existing SAP system
- Planning and execution of SAP improvement projects
- SAP Integration and interfacing with new/existing CBP systems
- End-user training assistance for new and existing SAP and SAP integrated systems functionality (FedTraveler for example)
- SAP Help Desk support

6.0.2 Status reporting will be accomplished on a weekly basis during project leadership meetings with the contractor and CBP management.

6.0.3 Expected deliverables consist of a monthly budget and staffing forecasts delivered to CBP Project management during monthly recurring review meetings.

6.0.4 Inspection and Acceptance of vendor services will take place upon timely receipt of appropriately prepared invoices and acceptance of hours requested for payment of those invoices by the CBP COTR and/or CBP management.

7.0 CONTRACTOR PERSONNEL

7.1 Key Personnel

7.1.1 In accordance with CBP policy all Key Personnel supporting CBP are designated as emergency/essential personnel.

7.1.2 DHS/CBP requires that the Contractor provide a Project Manager for this contract and that the Project Manager be designated as Key Personnel. The Project Manager will serve as a point of contact for the COTR and will serve as the interface between the government and the contractor employees. The Project Manager will provide centralized administration of all work performed under this contract.

7.1.3 The Contractor shall not make any personnel changes of Key Personnel unless an individual's sudden illness, death, or termination of employment necessitates such substitutions. In case of these occurrences, the Contractor shall notify the Contracting Officer promptly and submit documentation pertaining to the proposed substitution in writing at least fifteen (30) calendar days in advance of the proposed substitution.

7.1.4 The Contractor must provide a detailed explanation of the circumstances causing the proposed substitution. All resumes submitted for each proposed

substitution must have qualifications that are equal to or superior to the qualifications of the person being substituted to perform the work under this Work Statement.

7.1.5 The Contracting Officer and COTR shall evaluate the resume of each request to verify the qualifications of every new employee being assigned to this Work Statement.

7.2 Personnel relevant knowledge, skills, and abilities

7.2.1 This following is to inform potential contractors of the breadth and scope of skills that CBP may seek under this contract. CBP does not require the Contractor to establish these skill categories as labor categories.

7.2.2 Personnel assigned to perform on this Work Statement shall be required to possess a diverse set of skills. The labor categories shown in the paragraphs below are those that may be acquired in support of this effort. All personnel performing under this Statement of Work shall be able to perform the duties for their respective Government labor category positions described herein. CBP reserves the right to determine whether an individual's background and experience are sufficient to ensure adequate performance of this effort. All Contractor personnel shall be performing duties at: 1) a Government site, 2) via telework from employee home at on-site rates, or 3) at a Contractor site at off-site rates. CBP shall approve all performance locations, as well as reserving the right to choose the locations.

7.2.3 CBP is not restricting itself to acquiring only the labor categories listed in this document. More precisely, this is not an all-inclusive list of the support, which may be acquired. Specific education, experience and expertise may be required by the individual CBP program offices.

7.2.4 CBP has high volume, high performance and real-time applications operating in an environment that requires specialized, demonstrated management and technical expertise, as well as clearable personnel. In accepting Contractor personnel, CBP will place more value on specialized and demonstrated experience. The Contractor shall provide personnel with specialized and demonstrated experience in an environment similar and relevant to the CBP information technology environment. CBP will give consideration to certifications by recognized organizations in the skill area, to continuing education credits by nationally recognized institutions in related areas of study, and to relevant degrees. Progressive, unique, advanced and specialized experience that demonstrates value added qualifications are considered highly desirable. Personnel demonstrating ongoing development of technical expertise and teamwork capabilities are also highly desirable. Additionally, due to the critical mission and operations of the systems being supported, Contractor personnel who hold current (within the last 3 years) Secret and/or Top Secret

clearances, or current DHS/CBP Secret and/or Top Secret clearances, are preferable in order to ensure a smooth transition period.

7.2.5 The Contractor is expected to provide certified, trained, and knowledgeable technical personnel according to the requirements of this contract. Therefore, the CBP will not provide or pay for training, conferences, or seminars to be given to contractor personnel in order for them to perform their tasks. If it is determined during the performance of the Work Statement order that training, conferences, or seminars not specified in the Work Statement are required, only the CBP Contracting Officer may approve the training as specified in this document.

7.2.6 Labor Categories and Skill Levels

(i) GSA Category A - Project Executive
(ii) GSA Category C – Project Manager
(iii) GSA Category D – Senior Systems Analysts and Senior IT Specialists
(iv) GSA Category E – Senior Systems Analysts and Senior Systems Engineers
(v) GSA Category G – Systems Engineers
(vi) GSA Category H – Systems Analysts and Training Analyst
(vii) GSA Category I – Junior Analyst
(viii) GSA Category J – Journeyman Analyst
(ix) GSA Category K – Task Leader

Labor descriptions / skill levels are according to IBM GSA contract GS-35F-4984H, SIN 132-62, Appendix C, section C.1.

Further contract personnel requirements are found in Attachment A.

8.0 GENERAL INFORMATION

8.1 Disclosure of Information

8.1.1 Any information made available to the contractor by the government or its customers shall be used only for the purpose of carrying out the provisions of this contract. This information shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract.

8.1.2 In the performance of this contract, the contractor assumes responsibility for the protection of the confidentiality of government records.

8.1.3 The contractor will adhere to the requirements found in Part 24 of the Federal Acquisition Regulation, Protection of Privacy and Freedom of Information.

8.2 Technical Contact

8.2.1 The Customs and Border Protection technical contact person or Contracting Officer's Technical Representative (COTR) will be (b) (6) The COTR may be contacted at (202) (b) (6) or email at (b) (6) @dhs.gov.

8.2.2 All Contract administration matters will be handled by the Contracting Officer Michael Rebain at (202) (b) (6) or email at (b) (6) @dhs.gov.

8.3 Government Furnished Property

8.3.1 CBP will furnish all property, personal and real (space), to accomplish the tasks requested by the vendor under this SOW.

8.4 Contractor Furnished Items

8.4.1 The contractor shall provide for all services and personnel to perform those services to meet the requirement put forth in this SOW.

8.5 Procedures for Payment

8.5.1 Billing and payment shall be accomplished upon monthly submission to the COTR via email, of an invoice prepared by the vendor. Any terms and conditions, discounts, etc., will be considered by the COTR when found acceptable and beneficial to the Federal Government.

ATTACHMENT A: UNIQUE TECHNICAL AND PROGRAM REQUIREMENTS

A.1 INFORMATION TECHNOLOGY COMPLIANCY AND STANDARDS

A.1.1 SECTION 508 COMPLIANCE.

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

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

- 36 CFR 1194.22 – 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 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

- 36 CFR 1194.31 – 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.

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

36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall

procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards.

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

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

A.1.2 HOMELAND SECURITY ENTERPRISE ARCHITECTURE REQUIREMENTS.

(a) The Contractor shall ensure that all computer hardware and software designs conform to the DHS and Component enterprise architecture (EA), the DHS and Component technical reference models (TRM), and all DHS and Component policies and guidelines as promulgated by the DHS and Component Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA) such as the Component Information Technology Enterprise Principles and the DHS Service Oriented Architecture - Technical Framework.

(b) The Contractor shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and Component 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 Component 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 Component target architectures.

(c) Where possible, the Contractor shall use DHS/Component approved products, standards, services, and profiles as reflected by the hardware software, application, and infrastructure components of the DHS/Component 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 Components' 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/Component TRM/standards profile will be updated as technology insertions are accomplished.

(d) All developed IT hardware or software and recommended solutions shall be compliant with the HLS (Homeland Security) EA (Enterprise Architecture).

(e) Compliance with the HLS EA shall be derived from and aligned through the Component EA.

(f) 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.

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

A.1.3 SYSTEMS ENGINEERING LIFE CYCLE.

The Contractor shall be governed by and comply with the provisions of the DHS Systems Engineering Life Cycle Guide and Acquisition Management Policy (Directive 102-01). Any Contractor-specific best practices recommendations may be incorporated in a tailoring of the DHS Systems Engineering Life Cycle Guide. However, this action must be prior approved by the COTR.

A.1.4 USE OF WORKLENZ PRODUCT FOR REPORTING PURPOSES.

(a) The Contractor shall perform program and project planning and management duties to facilitate the development of the system and operational requirements for the task elements. This shall include the preparation of plans and schedules based on technical and project data; tracking program funds; scheduling and conducting technical and planning meetings; conducting project reviews; and preparing status reports. Additionally, these duties shall include entering program related information in CBP's WorkLenz tool.

(b) The WorkLenz tool is required to accomplish the following:

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

(c) Within seven (7) days of receiving WorkLenz Confidentiality Agreements from the COTR, Contractor shall have submitted all employee signed agreements. These agreements are required to protect the confidentiality provisions imposed by the Worklenz licensor.

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

(e) In agreement between the CBP COTR and the Contractor, paragraphs (a), (b), (c), and (d) of part A.1.4 of this SoW are not applicable to the Task/Delivery Order associated with this effort. The Contractor performs SAP System and other support services under this Task/Delivery Order for the Office of Administration which does not require the use of the WorkLenz System.

A.1.5 SECURITY REVIEW AND REPORTING.

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

(b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the Office of Inspector General, the Component's Chief Information Security Officer, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. 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/Component data or the function of computer systems operated on behalf of DHS/Component, and to preserve evidence of computer crime.

A.1.6 GENERAL RULES OF BEHAVIOR FOR USERS OF DHS/COMPONENT SYSTEMS AND IT RESOURCES THAT ACCESS, STORE, RECEIVE, OR TRANSMIT SENSITIVE INFORMATION

(a) Be advised that general rules of behavior shall apply to all Department of Homeland Security (DHS)/Component support Contractors who use DHS/Component systems and IT resources, such as laptop computers and portable electronic devices (PED) to access, store, receive, or transmit sensitive information. PEDs include personal digital assistants or PDAs (e.g., Palm Pilots), cell phones, text messaging systems (e.g., Blackberry), and plug-in and wireless peripherals that employ removable media (e.g., CDs, DVDs). PEDs also encompass USB flash memory (thumb) drives, external drives, and diskettes. The general rules of behavior are consistent with IT security policy and procedures within DHS Management Directive 4300.1 (Information Technology Systems Security), DHS Sensitive Systems Policy Directive 4300A, and the DHS 4300A Sensitive Systems Handbook. The rules of behavior shall apply to all Contractor employees at Component on-site and at any alternative off-site workplaces, as well as Contractor employees on official travel.

(b) Upon award of contract, the COTR shall provide each Contractor employee with a copy of the DHS/Component "General Rules of Behavior." The employee shall be required to sign and date an attached "Acknowledgement Form." The signed and dated forms shall be returned to the COTR within three (3) days of award or entry on-board.

A.2 CONTRACT MANAGEMENT REQUIREMENTS

A.2.1 EARNED VALUE MANAGEMENT SYSTEM

(a) In accordance with OMB Circular A-11, the Government will use Earned Value Management (EVM) to monitor tasks under CAPS. The Contractor shall provide EVM that

meets the criteria as defined in the current American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) Standard 748-2002, *Earned Value Management Systems*, approved May 19, 1998.

(b) Contracts and Task Orders in support of programs that have assets in the development, modernization, or enhancement phase will require the use of EVM to measure the cost, schedule, and performance of those assets against the established baseline. For contracts and task orders that are greater than or equal to $5M, the Government requires full compliance with the ANSI/EIA Standard 748 (2002) guidelines, with self-verification. For those contracts and task orders that are less than $5M but greater than or equal to $1M, the Government requires compliance to a specific subset of the ANSI-748 guidelines, with self-verification. For contracts and task orders that are under $1M annual cost, Earned Value Management is at the discretion of the Program Manager. The Contractor shall self-verify the compliance of its system. The Government reserves the right to apply the higher alternative EVMS standard to Prime Contractors with multiple contracts and task orders with a total cumulative value greater than $5M and greater than $1M. The Government reserves the right to obtain independent verification of a Prime Contractor's EVM system.

(c) In agreement between the CBP COTR and the Contractor, paragraphs (a) and (b) of part A.2.1 of this SoW do not apply to this Task/Delivery Order. The Contractors current support services Contract is performed under a Time and Materials basis for an ongoing, steady-state program, OA-SAP System, of which EVM is not a requirement.

A.3 SECURITY REQUIREMENTS

A.3.1 GENERAL SECURITY.

(a) All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. Contractor shall conform to all Component security policies.

(b) All services provided under this Work Statement must be compliant with DHS Information Security Policy, identified in MD 4300.1, "Information Technology Systems Security Program and 4300A Sensitive Systems Handbook".

(c) OMB-M-07-18 FDCC: In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.

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.

Security Certification/Accreditation

CBP Program Offices shall provide personnel (System Owner and Information System Security Officers) with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with the current version of the DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems Security Policies and Procedures Handbook HB-1400-05, and all applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series). During all SELC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools. An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO. While the ISSO performs security functions, the System Owner is always responsible for information system security (4300A). CBP will require any contracting firm that performs C&A and STE to put in place a legal firewall to prevent any conflicts of interest with DHS security work. This will ensure that the contractor has developed a robust Organization Conflict of Interest process to handle the separation of duties between the development of the security plan and the independent validation of its correctness. 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.

Interconnection Security Agreements

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

A.3.2 SECURITY REQUIREMENTS FOR UNCLASSIFIED IT RESOURCES.

(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 for each Component TO. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the Contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detailed in the approach **contained in the Contractor'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, 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 IT 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. DHS 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 the acquiring Component for approval by the TO Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The Contractor shall comply with the approved accreditation documentation.

A.3.3 CONTRACTOR EMPLOYEE ACCESS.

(a) Sensitive Information, as used in this clause, 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, 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, and insubordination, incompetence, or security concerns.

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

concerning the protection and disclosure of sensitive information both during and after contract performance.

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

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

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

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

(j) Contractor access shall 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) All Contractor employees supporting this contract shall be citizens of the United States, 48 CFR, 3052.237-71 (k) (1) which states: "Non-U.S. citizens shall not be authorized to access or assist in the development, operation, maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Organizational Element or designee, with the concurrence of the Office Of Security and Department's CIO or designee. In order for a waiver to be granted:

- 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.
- All required security forms specified by the government and any necessary background check must be satisfactorily completed. There must be a compelling reason for using this individual as opposed to a U.S, citizen. The waiver must be in the best interest of the Government."
- 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.

A.4 CONTRACTOR EMPLOYEES.

A.4.1 SECURITY CLEARANCES: PERSONNEL SECURITY BACKGROUND DATA

(a) All personnel employed by the Contractor and/or responsibility to the Contractor for the work performed shall either currently possess or be able to favorably pass a full field five (5) year background investigation required by the acquiring Component policies and procedures for employment. This policy also applies to any new personnel hired as replacement(s) during the term of this contract.

(b) **The Contractor shall submit within ten (10) working days after award** of the this contract a list containing the full name, social security number, and date of birth of those people who claim to have successfully passed a background investigation by DHS, or submit such information and documentation as may be required by the Government to have a background investigation performed for all personnel. The information must be correct and reviewed by the designated Component 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 Security0" 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 b a similar and equally qualified candidate as determined and approved by the Contracting Officer (CO) and the COTR. This policy also applies to any personnel hired as replacements during the term of the contract.

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

(d) 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, terminations, etc.); or upon final completion of the work effort. Failure of a Contractor to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports.

(e) The Contractor shall notify the COTR of any changes in access requirements for its personnel no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to another contract. The Contractor is responsible for the completion and timely submission to the COTR of the CF-242 for all departing contract personnel. Contractor shall provide the following information on behalf of their personnel to the COTR:

Full Name
Social Security Number
Effective Date

Reason for Change

(f) The Government may, at its discretion, direct the Contractor to remove any contract employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under this Work Statement. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee. Additionally, the Contractor shall not employ any person who is an employee of the United States Government, if that employment would, or would appear to cause a conflict of interest.

A.4.2 GOVERNMENT FURNISHED INFORMATION AND CONTRACTOR NON-DISCLOSURES.

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of the contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. **Contractor employees shall be requested to sign Non-Disclosure Statements that shall be provided by the COTR.**

A.4.3 OVERTIME.

The effort under this Work Statement is subject to the Services Contract Act of 1965. Contractor personnel may not work more than 40 hours a week without prior approval of the COTR. Approved overtime hours shall be invoiced at the normal hourly rate negotiated and agreed to for this effort.

In agreement between the CBP COTR and the Contractor, the COTR permits overtime work to be performed on an as needed basis determined by the Contractor PM. In accordance with this part A.4.5 of this SoW, all overtime will be billed at the normal hourly rates applicable to this Task/Delivery Order.

A.4.4 IDENTIFICATION BADGES.

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

A.4.5 CONTRACTOR IDENTIFICATION.

The Contractor shall ensure that its employees identify themselves as employees of their respective company while working on DHS/CBP contracts. For example, Contractor personnel shall introduce themselves and sign attendance logs as employees of their company, not as DHS/CBP employees. The Contractor shall ensure that their personnel use the following format signature on all official emails generated by DHS/CBP computers:

Name
Position or Professional Title
Company Name
Supporting the XXX Division/Office...
US Customs and Border Protection
Phone
FAX
Other contact information as desired

A.4.6 MANDATORY AND OTHER TRAINING.

(a) **SECURITY AWARENESS AND RECORDS MANAGEMENT TRAINING.**

Security Awareness and Records Management training for all agency personnel, Contractor employees, and other users is mandatory. The training will involve information regarding the risks to agency information and information systems and their obligations in complying with agency information security policies and procedures.

(b) A key objective of an effective IT security training program is to ensure that each employee understands his or her roles and responsibilities and is adequately trained to perform them. The DHS cannot protect the confidentiality, integrity, and availability of its IT systems and the information they contain without the knowledge and active participation of its employees in the implementation of sound security principles.

(c) The Contractor shall be responsible for ensuring that its personnel received the requisite security training depending upon individual work effort and/or roles and responsibilities. Contractor personnel shall be required to complete one or more levels of DHS security training: 1) initial training in IT security concepts and procedures, 2) annual refresher training (if the effort duration is greater than 12 months), and 3) role-based training. Role-based training may be required for Contractor personnel who are involved in IT efforts and who are required to perform any IT security responsibilities.

(d) DHS policy requires Contractors/Subcontractors receive security training commensurate with their responsibilities for performing work under the terms and conditions of their contracted agreements. The contractor shall ensure that each contractor/subcontractor employee has completed the necessary DHS/Component Computer Security Awareness Training prior to performing any work, and, thereafter, completing a DHS/Component – specified fiscal year refresher course during the period of performance under this Statement of Objectives.

(e) The Contractor shall maintain a listing by name and title of each contractor/subcontractor employee working under this Work Statement who has completed the required training. Any additional security training completed by the Contractor or subcontractor employees shall be included in the first Monthly Status Report. Any revisions to this listing as a result of staffing changes shall be submitted in the next Monthly Status Report.

A.4.7 TRAVEL

Contractor personnel may be expected to conduct temporary duty trips in support of the efforts described in the Work Statement. In the event that such travel is required, both the COTR and the Contracting Officer must approve such travel in advance. CBP will reimburse all allowable travel costs. All travel costs are subject to Federal Acquisition Regulation Subpart 31.205-46, Travel and the Federal Travel Regulation. Unallowable costs include such items as: 1) mileage costs in the use of a privately owned vehicle for to and from place of work; 2) parking fees; 3) fines of any kind; and 4) air fare tickets above the Government authorized amount.

A.4.8 PROTECTION OF GOVERNMENT INFORMATION AND DATA.

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

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

A.4.10 EMPLOYEE CONDUCT.

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

A.4.11 CONTRACTOR INPUT AND TRACKING.

(a) The Contractor shall require that each employee under the contract has:

(1) entered information into the CBP web-based phone system

(2) provided information to be entered into the CBP Contractor Tracking System.

(b) In accordance with U.S. Customs and Border Protections Security Policy No. OIT SEC 2.16 "OIT Policy for Centralized Contractor Tracking" The Contractor is responsible for ensuring that all on-boarding and separating employees comply with this directive by immediately supplying the Contract Officer's Technical Representative (COTR) with the relevant information required to satisfy this directives requirements.